A BZ Media Publication

SD Times

SOFTWARE DEVELOPMENT

The Industry Newspaper for Software Development Managers

MARCH 1, 2007 • ISSUE NO. 169

www.sdtimes.com • $7.95

Standish Group Report: There's Less Development Chaos Today

BY DAVID RUBINSTEIN

Software development shops are doing a better job creating software than they were 12 years ago, according to figures contained in the as-yet unreleased 2006 Chaos Report from The Standish Group.

The new report, details of which were previewed with SD Times, reveals that 35 percent of software projects started in 2006 can be categorized as successful, meaning they were completed on time, on budget and met user requirements. This is a marked improvement from the first, groundbreaking report in 1994 that labeled only 16.2 percent of projects as successful; that report galvanized an industry of development tools vendors selling everything from requirements management solutions to modeling tools and turned software architecture into a cottage industry.

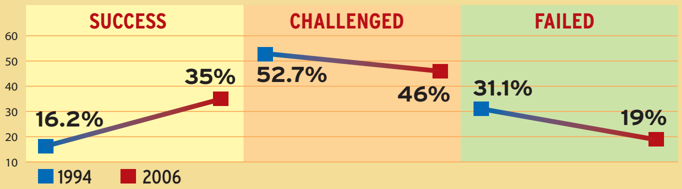
Further, the 2006 study shows that only 19 percent of projects begun were outright failures, compared with 31.1 percent in 1994. The 2006 report is the sixth published by The Standish Group, and chairman Jim Johnson said that with the exception of a lapse in 2004, "we've seen consistently better software projects."

Projects described as challenged, meaning they had cost or time overruns or didn't fully meet the user's needs, declined to 46 percent in 2006 from 52.7 percent in 1994.

Johnson cited three reasons for the improvement in software quality—better project manage-

continued on page 19 ►

GETTING BETTER ALL THE TIME



A project is considered a success if it's delivered on time, on budget and meets requirements. It is considered challenged if it's late, costs more than projected and doesn't meet all the requirements. It is said to have failed if it gets canceled before completion or is not deployed by the end user.

Source: The Standish Group

The alliance must make its work known, says Oracle's Sullivan.

Liberty Alliance Struggles With Its Own Identity

BY ALEX HANDY

The Liberty Alliance is having an identity crisis. The group of vendors and independent developers that came together in 2001 to build standards and practices for digital identity management will be changing its tactics in 2007, due to what has been described as a proliferation of fear, uncertainty and doubt in the marketplace.

The 6-year-old project will attempt to open its processes and discussions to the public in the coming year, something that it has not done in the past. The alliance will also be seeking out other identity management projects to foster collaboration and interoperability.

"From a personal perspective, adoption [of Liberty Alliance standards and protocols] went a little bit slower than I anticipated," said Jason Rouault, vice president of the Liberty Alliance and

continued on page 24 ►

OSGi, JCP Tussle Over Component Support in Java

Critics decry effort as a rubber-stamp move

BY ALEX HANDY

The technology already works; it's undergone four major revisions, in fact. So why is Sun Microsystems upset about JSR 291's progress on the road to ratification? Because, the JSR's detractors claim, the work done on the proposal for Dynamic Component Support for Java SE was performed outside of the JCP.

Jim Colson is chief architect at IBM client software, and he's been

continued on page 29 ►

A Site That Can't Be Hacked?

ScanAlert's claim called outrageous; retailers see gains

BY JENNIFER DEJONG

It's not quite ubiquitous, but the HackerSafe seal of approval is quietly gaining ground on the Web, with more than 70,000 sites sporting the black-and-white logo with the green light.

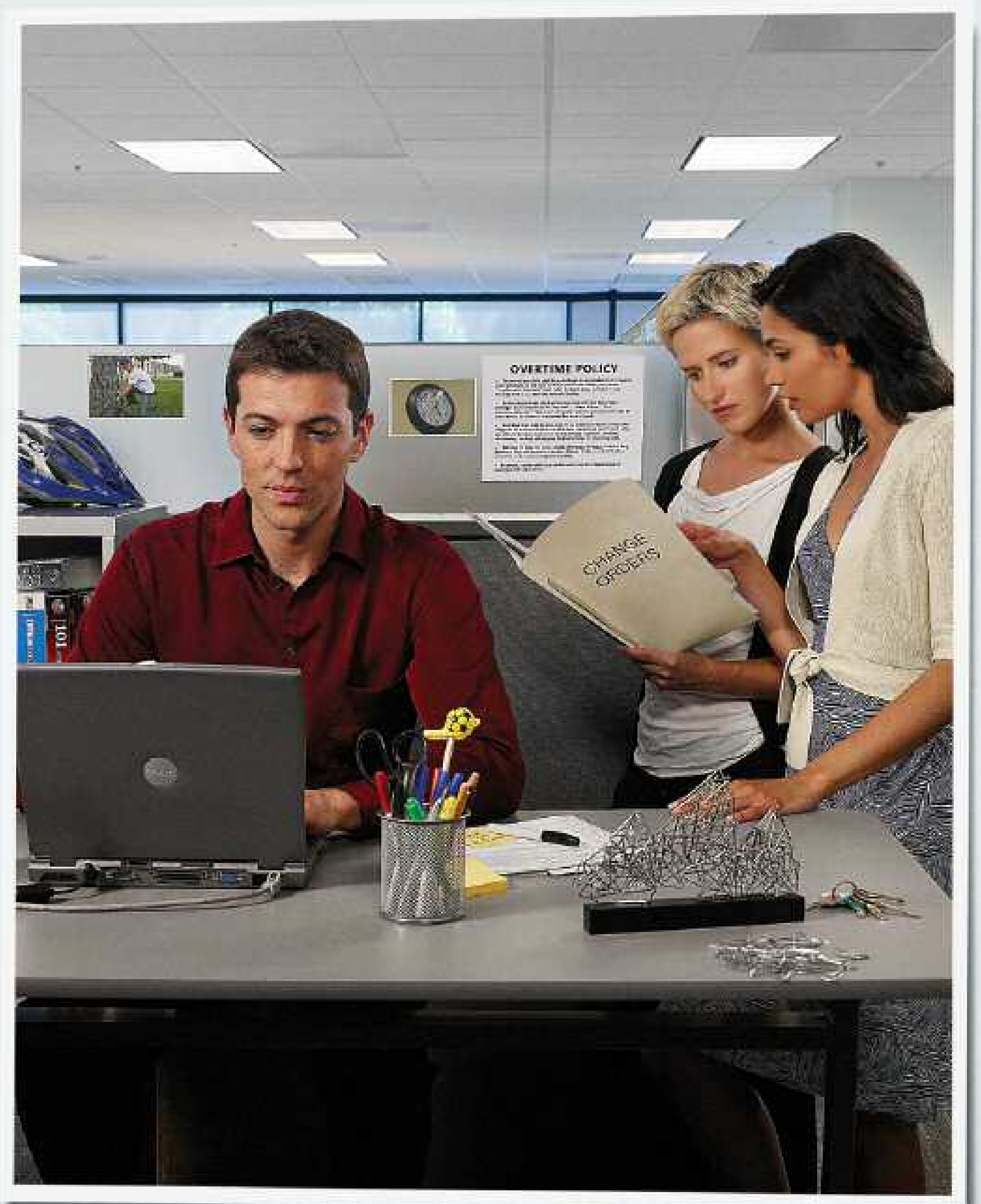
Aimed at giving hesitant online shoppers the confidence to make a purchase, the HackerSafe mark is intended to settle once and for all the question of whether it's safe to use a credit card online. But among application security professionals, the seal raises many more questions than it answers: Who is the organization behind the mark? How can a company that sells security services also call itself a certifying authority? And, most perplexing, at a time when security breaches continue to make headline news, how can anyone guarantee a site is safe from hackers?

"It is an outrageous claim," said Roger Thornton, chief technology officer for Fortify Software, which sells source code analysis and other application security tools. Even if a development team adopts secure practices across the board, from requirements, to coding, testing and deployment, he said, "no one can say their code is unhackable."

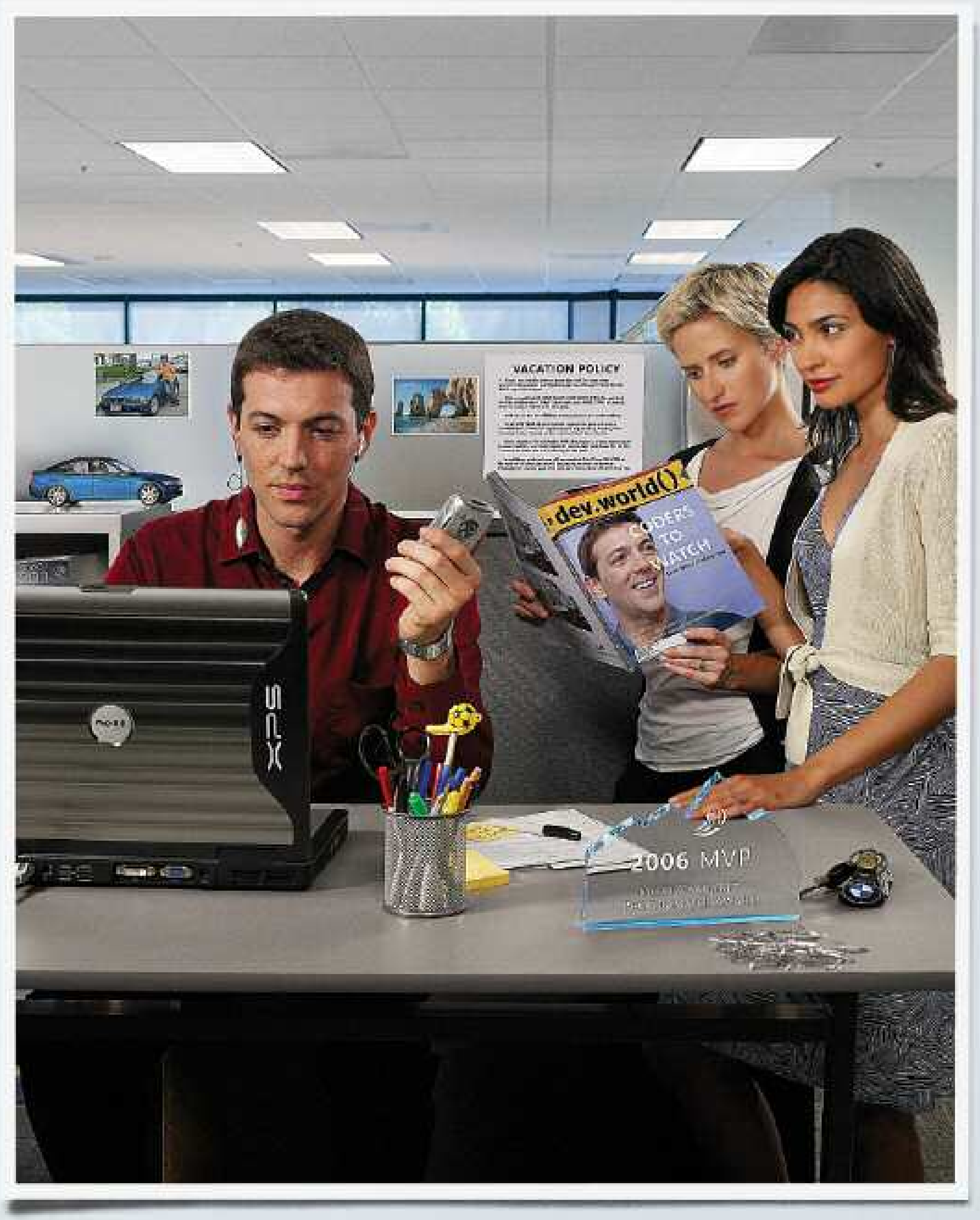
The company behind the HackerSafe certification mark

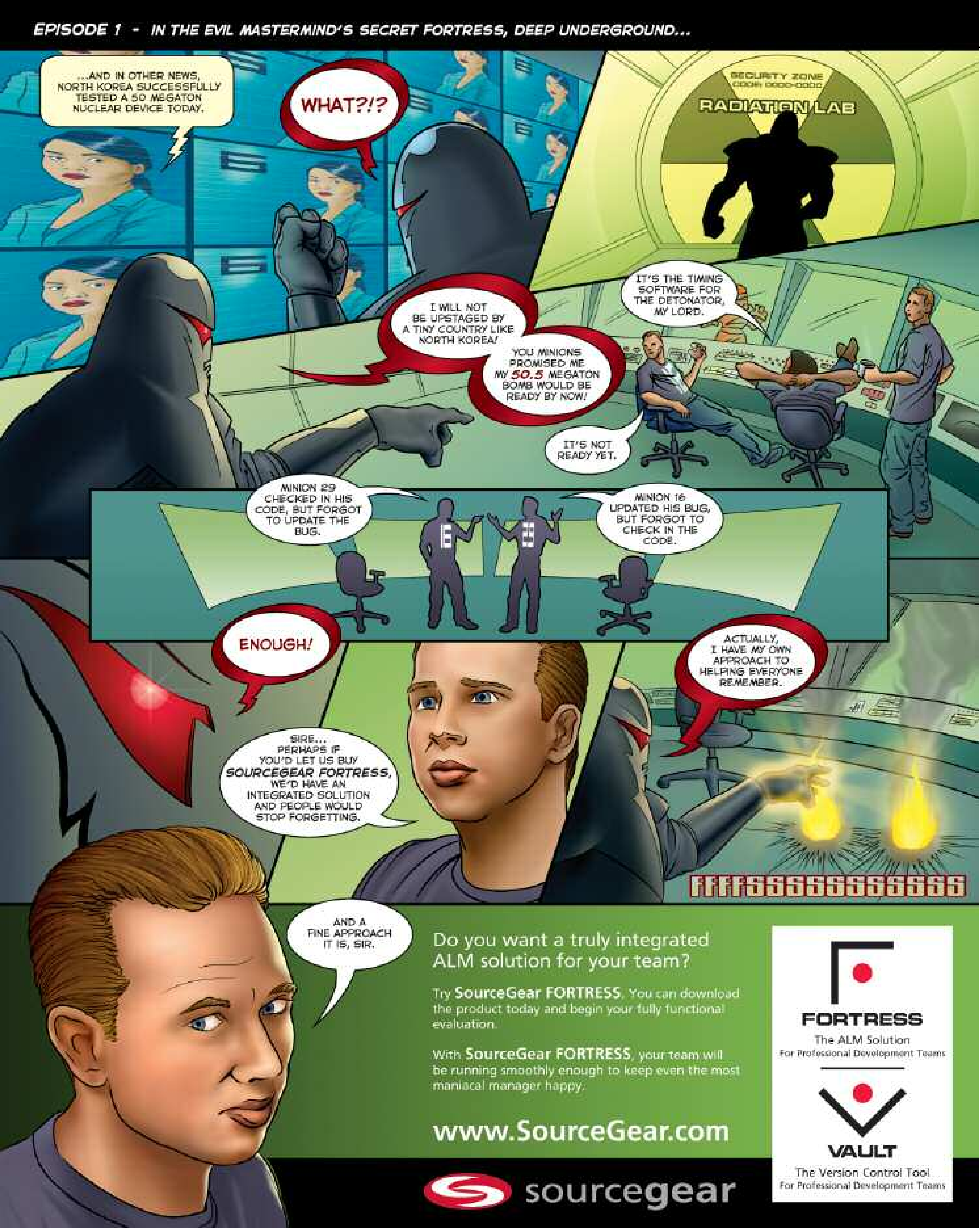
continued on page 30 ►

IN THIS ISSUE



Visual Studio® 2005.
The difference is obvious.


VACATION POLICY
dev.world()
CODERS TO WATCH
XPS
2006 MVP


EPISODE 1 - IN THE EVIL MASTERMIND'S SECRET FORTRESS, DEEP UNDERGROUND...
...AND IN OTHER NEWS, NORTH KOREA SUCCESSFULLY TESTED A 50 MEGATON NUCLEAR DEVICE TODAY.
WHAT?!?
RADIATION LAB
I WILL NOT BE UPSTAGED BY A TINY COUNTRY LIKE NORTH KOREA!
YOU MINIONS PROMISED ME MY 50.5 MEGATON BOMB WOULD BE READY BY NOW!
IT'S THE TIMING SOFTWARE FOR THE DETONATOR, MY LORD.
IT'S NOT READY YET.
MINION 29 CHECKED IN HIS CODE, BUT FORGOT TO UPDATE THE BUG.
MINION 16 UPDATED HIS BUG, BUT FORGOT TO CHECK IN THE CODE.
ENOUGH!
SIRE... PERHAPS IF YOU'D LET US BUY SOURCEGEAR FORTRESS, WE'D HAVE AN INTEGRATED SOLUTION AND PEOPLE WOULD STOP FORGETTING.
ACTUALLY, I HAVE MY OWN APPROACH TO HELPING EVERYONE REMEMBER.
FFFSSSSSSSSSSS
AND A FINE APPROACH IT IS, SIR.
Do you want a truly integrated ALM solution for your team?
Try SourceGear FORTRESS. You can download the product today and begin your fully functional evaluation.
With SourceGear FORTRESS, your team will be running smoothly enough to keep even the most maniacal manager happy.
www.SourceGear.com
sourcegear
FORTRESS
The ALM Solution
For Professional Development Teams
VAULT
The Version Control Tool
For Professional Development Teams

Microsoft Shares Its SaaS Odyssey

Offers insight, guidance on how it created its reference implementation

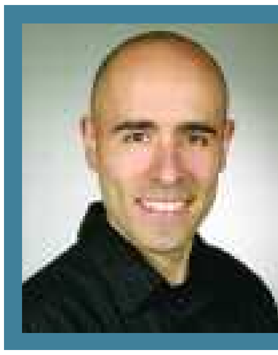
BY DAVID WORTHINGTON

Microsoft has given software architects a candid look at the challenges it faced as it developed its software as a service (SaaS) platform reference application. The source code of the application, dubbed Litware HR, is available at CodePlex under Microsoft's Permissive License to demonstrate how to use the platform in the context of that application. "Litware" joins "Northwinds" and "Contoso" as the latest in the series of dummy companies that Microsoft applications use for demonstration purposes.

White papers and other prescriptive architectural guidance on the key principles of SaaS began showing up on MSDN a year ago, and Microsoft says that Litware HR is the embodiment of that guidance. The company expects to detail how Microsoft engineers built the Litware reference application at a later date on its Skyscrapr.net community site.

"The main reason for the delay [between white paper and reference application] was…the direction of effort toward Vista and Office releases," speculated Chris Howard, vice president and service director at Burton Group. "Microsoft has been doing its homework to test the validity of its strategy before releasing something prematurely. Couple this with the fact that many customers haven't gotten their arms around developing SaaS-based apps. SaaS appears to be a new strategic direction for [Microsoft], but is generally misunderstood or siloed into specific functional areas," he said, referring to Salesforce.com for CRM as an example.

Gianpaolo Carraro, director of Microsoft's solutions architecture group, explained the company's determination to offer ISVs such extensive guidance: "It is important to show the journey as well as to show the destination."



'It is important to show the journey as well as to show the destination.'

—Gianpaolo Carraro, director of Microsoft's solutions architecture group

'ARCHITECTS IN ACTION'

To that end, Microsoft is publishing the behind-the-scenes meetings, processes and artifacts that it used while fleshing out Litware HR, in a series called "Architects in Action." The premise of the series is that it is possible to slay the "three-headed monster" Microsoft says haunts all SaaS ISVs—the heads being customization, multi-tenant efficiency and scalability.

In the world of SaaS, scalability means that you must use resources as efficiently as possible to make a profit, according to Carraro.

Examples of this are partitioning large databases or sharing pooled resources. "There must be a high density of customers for hardware. You are hosting the application and users' data of customers and tenants," said Carraro. For customizing desktop applications, which are run as a single instance for all customers, "a vendor cannot have the liberty to make individual changes [in an application for a specific customer], without impacting other customers," Carraro explained. But metadata can be used to customize details for each tenant, while running a single instance of an application. Microsoft has engineered runtimes to process this metadata, adding another layer to the application, Carraro said.

The idea behind multi-tenant efficiency is to offer services at a lower price than traditional enterprise software is offered, through economy of scale—effectively a one-to-many solution. Microsoft's Carraro acknowledged that a multi-tenant architecture has a longer time-to-market, and vendors must pay what he called a "tax" at the beginning because of a higher isolated cost per tenant. According to Carraro, cost-saving efficiency is realized over the long term, after the tenant base grows.

Burton Group's Howard observed: "Unlike a standalone SaaS application, the broader vision of SaaS is of an enterprise development option where logic spans organizational limits—that is, creation of a composite application whose logic is hosted in multiple places inside and outside, combined with existing applications [such as COTS, custom and OSS]. It's not that the platform, or architecting SaaS apps in general, is complicated; it's the challenge of refactoring existing enterprise logic so that it can be recombined or sliced off, and hosted elsewhere as a service."

Litware's logic is composed of externally hosted Windows workflow services. Workflows are hosted internally and externally, by vendors, in the .NET 3.0 application architecture.

".NET 3.0 can forklift pieces from one side to another without having to rearchitect the application whenever those pieces are moved. The reference application emphasizes the core business model and deliberately leaves this out," said Howard.

Howard concluded, "I suspect this is the first iteration of a more sophisticated SaaS evaluation from [Microsoft], future versions of which will be more prescriptive about exercising the .NET 3.x programming model." ∎

ALM Inches a Step Closer to Application Security

Borland's Gauntlet partners are a first sign vulnerability testing has arrived

No one knows where app security should go in the development cycle, says Forrester's Schwaber.

BY JENNIFER DEJONG

Application security hasn't been a high focus area for ALM tool makers, but Borland Software may be showing signs that a change is finally afoot.

When the company announced its Open Application Lifecycle Management strategy earlier this year, it named three application security partners: Cenzic, Fortify and Klocwork. "I am not surprised that [Borland is] pushing security as a big issue," said Ovum analyst Bola Rotibi. It's likely to become a big issue for all ALM tool makers going forward, she said.

Included in Borland's Open ALM announcement was the launch of Gauntlet. The automated build and testing tool is based on technology Borland acquired when it bought Gauntlet Systems last May. Designed to work with Borland's Lifecycle Quality Management (LQM) tools—for project management, requirements definition, quality management and change management—Gauntlet provides development teams with an efficient way to subject code to various forms of analysis before it is checked in for a build, noted Forrester analyst Carey Schwaber.

For instance, by plugging Cenzic's Hailstorm into Gauntlet, a team could conduct black-box tests on its code, simulating actual attacks in order to pinpoint holes a hacker might exploit. In the same fashion, Fortify's SCA or Klocwork's K7 could be used to analyze source code for vulnerabilities.

Asked whether Borland's emphasis on application security is a sign that black-box testing and source code analysis are likely to become integral parts of the ALM process and of the ALM tool set, Borland vice president of product marketing Marc Brown said security is just one among several quality issues.

But Borland agrees that, among ALM tool makers in general, security aspects of quality have not made their way into application life-cycle discussions. "But to be successful with application security—or anything else, for that matter—you have to ensure that discipline is woven into daily practices," said Borland director of development solutions Rob Cheng. Cenzic vice president of marketing Mandeep Khera agreed. "You have to catch security vulnerabilities earlier in the cycle." To accomplish that, application security testing must become part of the ALM process, he said.

WHERE DOES IT FIT?

One reason why that hasn't happened yet is that it is difficult to figure out just where application security fits, said Schwaber. "No one knows where in the development cycle it should go." It's not clear whether it's the responsibility of developers or testers, or that of the information security group, she said. She doesn't believe Borland is promoting the appli-

continued on page 13 ▸

NEWS BRIEFS

COMPANIES

The SOA Consortium has been formed to promote adoption of service-oriented architecture. Founding sponsors are **BEA Systems**, **Cisco**, **IBM** and **SAP**; participating companies include **Avis Budget Car Rental**, **Bank of America**, **Hewlett-Packard**, **Object Management Group** and **WebEx Communications**. The mission of the consortium is built on the notions that SOA is key for the 21st century enterprise; that achieving the benefits of SOA requires significant changes for both IT and business executives; and that SOA is perceived by business executives as an IT integration story, not a business agility story. Input from by-invitation CIO summits run by the group are intended to validate the mission, according to the group.

NEW PRODUCTS

IBM in mid-February announced its **Open Client Solution**. This package of software, which includes the Lotus suite of productivity tools and Mozilla Firefox, is an effort to build out the applications that businesses need in a manner that is compatible with both Windows and Linux. IBM internally deployed Linux-based desktop systems to test this solution, in what the company is calling the world's largest enterprise desktop deployment. IBM also announced **FileNet**, an information archival system aimed at solving the data retention and informational awareness needs of companies. FileNet is a strategic information-on-demand system that the company acquired in October 2006 through an acquisition. The software aims to catalog and make available the various types of information and content businesses use . . . Dundas Software has unveiled **Dundas Chart for SharePoint**. Dundas Chart is deployed standalone in Microsoft Office SharePoint Server (MOSS), independent of Visual Studio, providing both .NET programmers and regular users with charting capabilities. AJAX interactive features, data binding, integration with the MOSS Business Data Catalog and Excel services are supported . . . Liberty BASIC is teaching the basics of BASIC with an interactive programming environment called **Run BASIC**. Don't dust off your Tandy just yet—it is all browser-based. Run Basic hosts sample applications, provides lessons and executes users' code during Web-based sessions. The service is free of cost and suitable for ages 9 to 99 . . . **ExtremeDB Fusion**, which brings together the benefits of on-disk and all-in-memory data management into a single embedded database system, was released in February by McObject. This allows developers flexibility in calling some data transient, to be managed in memory, while selecting on-disk storage for other types of records, all with a simple schema declaration . . . Macraigor Systems has released its **Eclipse + GNU Tools Suite**, which combines Eclipse 3.2.1 with the binutils, gcc, gdb and gdb-tui tools from GNU and adds ODC Remote, an interface between the Eclipse framework, the gdb debugger and a Macraigor on-chip debug device. Macraigor is joining the Eclipse Foundation as an add-in provider.

UPDATES

CodeGear in February released two new versions of its **Delphi** rapid application development IDE. The first, Delphi 2007, brings Windows Vista support to the environment. Delphi 2007 also adds AJAX functionality to the mix. Delphi for PHP was also released in February, and brings visual application development tools into the world of PHP . . . Aonix has released **ObjectAda Real-Time Raven 8.3** for developing PowerPC-based embedded systems. This release of ObjectAda implements the Ravenscar profile, a restricted subset of the Ada runtime environment for applications requiring either safety-critical certification or simply a predictability of performance. Aonix has made this environment available to developers with no-cost Eclipse plug-ins.

PEOPLE

Device data management software provider Encirq has named **Deborah Goslin** as CEO. Goslin succeeds founder **Mark Vogel**, who will remain on the board and act as a strategic adviser. Goslin brings more than 25 years of experience in high-tech sales. ▮

Microsoft's Doc Format Conversion Utility Done

BY DAVID WORTHINGTON

The Microsoft-sponsored open source project tasked with developing an Open Office XML (OOXML) to Open Document Format (ODF) conversion utility reached the 1.0 milestone on Feb. 2. The OpenXML Translator add-in is compatible with Office XP and Office 2003, and will be bundled into a future version of Novell's OpenOffice distribution, per the technology exchange agreement between Microsoft and Novell. But the jury is still out on whether this technical bridge is sound.

Meanwhile, Sun Microsystems has jumped into the fray, and is developing a plug-in of its own for its StarOffice 8 productivity suite. The plug-in will enable two-way conversion between ODF and Microsoft Office 2003's .DOC format.

Interest in the open-source OOXML conversion utility has been high since its release: It is SourceForge's ninth-most-active project, based on user activity, including downloads. Some contributors were enlisted by Microsoft to ensure the software's timely arrival after development began in July 2006. Project members produced a two-way OOXML and ODL document translator that is available in Dutch, English, French, German and Polish versions.

Clever Age, a French consulting company, assigned seven full-time developers to the project from its headquarters in France and its Polish subsidiary. Dialogika, a Germany-based ISV, and Aztecsoft, an India-based company, tested the bits. Clever Age did all of the development work and received technical assistance on the OOXML specification from Microsoft.

Project leader Jean Goffinet from Clever Age expected the open source community to be more engaged in the project. "I must admit that we expected more interest [in] the project during its development phase," he told SD Times in an e-mail, "but the community remained very cautious. However, we managed to finish the first stage in time. Hopefully the community will grow now that a first official release was published."

Some Microsoft partners are heartened about the add-in's release, but some end users are unimpressed by its accuracy. "The translator project is the kind of support customers expect and deserve. This allows a company like ours to integrate solutions more easily for the interoperability requirements of our international customers," said Michele Balbi, president of Teorema Engineering Group, an IT systems integrator in Italy and a Microsoft Gold-Certified partner.

CONVERTER A 'DUD'?

Naysayers claim that the translator doesn't work; and at least one blogger has attempted to demonstrate this.

Zaine Ridling, author of the "The Great Software List," published a February entry with error dialogs in support of this view. The screenshots purported to demonstrate that document elements of a large OOXML file were lost during a conversion from the default Word 2007 format to ODF. "The Microsoft-funded ODF converter for Word 2007 already is proving to be a dud, failing to properly convert any of my DOCX documents properly to ODF. (None were created using Compatibility Mode in Word 2007)," Ridling wrote in his blog.

SD Times has been unable to verify that Ridling was using the final version of the converter, despite attempts to contact him.

Chris Swenson, an analyst with NPD Group, waved off the claims of problems with the utility, saying, "I would rather use Microsoft's converter to their format than the other way around." He further noted, "The vast majority of people that are creating Word documents will leave them in native format."

The second phase of the Microsoft/SourceForge project expands the scope of conversion to spreadsheet and presentation software. A technical preview of add-ins for Excel and PowerPoint will be made available in May 2007. ▮

Borland Weaves Silk Into Open ALM Strategy

BY JEFF FEINMAN

Borland Software is trying to bring more smoothness to its Silk. The company has spun a slew of new capabilities into the three main products that make up its quality assurance suite, Borland Silk, as it weaves together its Open ALM strategy, which was unveiled in January.

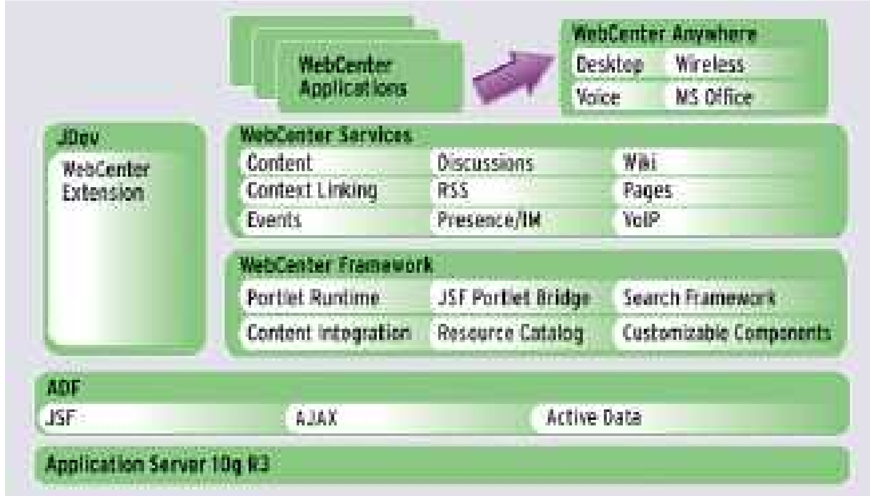
Borland officials said that the most important enhancements were made to SilkCentral Test Manager. The company's test management tool has been equipped with an Eclipse-based testing client that provides testers with a standalone application on their desktop for manual testing.

Brad Johnson, Borland's product marketing director, said that customers expressed the need for a more user-friendly client, with test-to-code impact analysis that lays out each step of manual testing.

SilkPerformer, the company's load-testing product, now includes Java Management Extensions—a standard API for tools that manage and monitor devices and applications. SilkPerformer also has a new plug-in to the Eclipse IDE. Meanwhile, the SilkTest automated functional testing tool adds new collaboration capabilities enabled by Windows Vista. Johnson said that many software vendors that are Borland customers have built applications on Windows Vista, and SilkTest allows them to record and run automated functional tests in that environment.

"This announcement continues to improve the alignment between development organizations and quality assurance organizations," Johnson said. "Typically…there's very often a big rift in communication between [QA] teams and development teams that are actually delivering software code."

Borland defines its Open ALM concept as offering customers the ability to use any combination of life-cycle tools, whether commercial or open source, and catering to a broad range of platforms. ▮



Source: Oracle

The Oracle WebCenter Suite offers developers access to a variety of services for building enterprise mashups and composite applications.

Oracle Joins the Mashup Parade With WebCenter Suite

BY P.J. CONNOLLY

Oracle released its latest answers to the questions of data integration, search and Web 2.0 in February, with the unveiling of an update to Oracle Secure Enterprise Search 10g, and the new Oracle WebCenter Suite and Oracle Data Integrator.

The WebCenter Suite is a key part of Oracle's Fusion strategy for applications and middleware; the company calls the suite "the foundation of the user interface" of Fusion applications.

The heart of the WebCenter Suite is the WebCenter framework, which allows developers to implement role-based customization and rapid, modular content creation in JavaServer Faces and Java EE Web applications. The company claims a first among major vendors, by incorporating WSRP (Web Services for Remote Portlets) 2.0 support into WebCenter Suite.

The WebCenter framework is a declarative development environment, optimized for hosting standards-based components and providing a content integration layer, based on JSR 170, that allows the use of multiple content repositories. Portlets compliant with the Java portlet specification will work with WebCenter, and mobile users are supported with the framework's built-in multichannel support.

WebCenter Services is a collection of prefabricated Web 2.0 services designed to help enterprises enter the world of so-called application "mashups." Content management, discussion threading, instant messaging, online awareness, secure search and wiki services enable collaboration and information sharing.

The WebCenter Studio ties into Oracle JDeveloper and provides developer access to the WebCenter framework and services. It includes wizards for a variety of common tasks, such as building and consuming portlets, securing an application, and creating a data control for accessing a content repository. Veteran developers may find this reduces the amount of code they need to write, while newcomers have always appreciated a leg up.

In another Fusion Middleware development, Oracle announced the availability of Oracle Data Integrator, based on technology from the company's acquisition of Sunopsis, and is designed for high-performance use with database, data warehouse and other applications from vendors such as IBM, Microsoft, Sybase and Teradata.

Data Integrator replaces conventional approaches to ETL (extract, transform and load) operations that require a separate machine to perform the data manipulation; instead, it performs the transformation on either the source system or the target.

WHO ARE YOU? WHAT DO YOU SEEK?

Meanwhile, Oracle's updated enterprise search package, which runs on Linux, Unix and Windows, was updated with a framework offering extensible authentication, authorization and identity management that supports third-party identity management schemes, including Microsoft Active Directory, Novell eDirectory, OpenLDAP and Sun Java System Directory Server.

Oracle Secure Enterprise Search 10g release 10.1.8 also adds federated search capabilities, including a framework that allows Oracle search servers to "farm out" search requests to other Oracle search instances, whether they're embedded into an application or are standalone servers.

Secure Enterprise Search 10g can peruse a variety of data sources with a single query, including EMC Documentum Content Server DocBases, FileNet Content Engine object stores, IBM Lotus Notes/Domino databases, Microsoft Exchange and SharePoint. ∎

Introducing:

TestTrack® TCM

The ultimate tool for test case planning, execution, and tracking.

Seapine ALM Solutions:

TestTrack Pro
Issue & Defect Management

TestTrack TCM
Test Case Planning & Tracking

Surround SCM
Configuration Management

QA Wizard
Automated Functional Testing

Seapine Software™

How can you ship with confidence if you don't have the tools in place to document, repeat, and quantify your testing effort? The fact is, you can't. **TestTrack TCM can help.**

In TestTrack TCM you have the tool you need to write and manage thousands of test cases, select sets of tests to run against builds, and process the pass-fail results using your development workflow.

With TestTrack TCM driving your QA process, you'll know what has been tested, what hasn't, and how much effort remains to ship a quality product. Deliver with confidence—be a testing superstar!

- Ensure all steps are executed, and in the same order, for more consistent testing.
- Know instantly which test cases have been executed, what your coverage is, and how much testing remains.
- Track test case execution times to calculate how much time is required to test your applications.
- Streamline the QA > Fix > Re-test cycle by pushing test failures immediately into the defect management workflow.
- Cost-effectively implement an auditable quality assurance program.

Download your **FREE** fully functional evaluation software now at **www.seapine.com/sdttcm** or call 1-888-683-6456.

SD WEST 2007 See us at **Booth 502**

JackBe's Presto Jazzes Up Look of SOA

BY DAVID WORTHINGTON

Amidst all the talk of the ins and outs of SOA, JackBe is voicing its concern that not enough attention is devoted to the end-user experience. Making these services easy on the eye is the aim of JackBe's Presto Rich Enterprise Application (REA) platform, which couples SOA with AJAX. Presto's beta bits are currently undergoing testing, and the finished product is expected to ship around March.

According to Jerrold Prothero, JackBe's resident user interface expert, "Presto's AJAX UI layer is derived from Overwatch. [Overwatch is an interface JackBe is developing for the U.S. Defense Intelligence Agency.] New UI layers will be created on a per-sector basis, corresponding to users' needs."

In Prothero's opinion, user interfaces should be designed from the user on out. That way, he claimed, the user base is built into the product. In his opinion, Web interfaces are playing catch-up to the desktop, and a good Web interface can make SOA more assessable.

Presto is a layer that rests on top of SOA that provides a back-end structure and AJAX interface to connect to Web services. JackBe has keyed in on three primary business requirements for Presto REA to address: service governance, empowerment and reliability.

Five platform components provide a means to those ends. The Enterprise Service Director tackles governance management, providing access control, handling authentication and permissions, and trusted services through a mediation gateway. Both internal and external services pass through the gateway layer; databases, WS/REST and .NET are supported.

Another component, an enterprise "mashup" server, lassos together disparate services to create hybrid Web applications. Users can dynamically combine Web services with AJAX to create widgets, or views, to save and share with others.

JackBe's AJAX service bus is the mechanism that puts the "asynchronous" in AJAX, designed to be scalable and reliable, and to offer secure, bidirectional messaging between client and server, support for push-based events and "once-and-only-once" message delivery.

The final two pieces of Presto are geared toward developers. Advanced developers may find more utility in the NQ Ajax Framework, a runtime development framework that uses an XML-based schema-driven mark-up language.

NQ Studio is a visual, browser-based WYSIWYG studio, designed for nonprogrammers.

FOCUS ON GOVERNANCE

"There are scores of new products designed to accelerate AJAX development and client-side mashup of Web services," said Ron Schmelzer, senior analyst with ZapThink. "What makes JackBe's Presto platform unique is its central focus on SOA service governance. JackBe clearly understands that governance, scalability and reliability are critical factors for enterprises as they leverage SOA and AJAX to create the next generation of rich enterprise applications." ∎

Progress Software Ups the Ante With OpenEdge

New version of its flagship platform ships with updated 4GL, database management, Eclipse

BY DAVID WORTHINGTON

By its own admission, Progress Software has been a "quiet company." It may even be one of the largest companies you've never heard of—its flagship OpenEdge platform has generated more than US$5 billion in partner revenue in the past two years. Determined to make more noise, Progress is gearing up to release version 10.1B of OpenEdge to service its core customers and woo Eclipse developers.

OpenEdge is a 4GL application infrastructure for developing, managing and deploying business applications. It ships with development tools and a deployment environment, interacts with databases, and has lifecycle management facilities. The IDE is now Eclipse 3.2-based—familiar territory to a pool of 2.27 million software developers, according to IDC's estimate published in August 2006.

Open Edge can now handle enterprise-sized databases with large tables that contain trillions of rows. The company claims a simultaneous user ceiling of 20,000 on linear scalability, with little or no exponential decay until that point.

ABL EXPANDED

OpenEdge's proprietary 4GL Advanced Business Language (ABL), used to codify business logic, has been expanded to be more object-oriented. This, Progress claims, makes for better interoperability with other object-oriented applications and more code reuse.

OpenEdge runs on Linux, Unix and Windows. The new version allows the use of 64-bit data formats in software, and 64-bit PowerPC processors on the hardware front.

Jeffrey Hammond, a senior analyst at Forrester Research, said that OpenEdge 10.1B will mollify developers who could otherwise abandon the platform for a 3GL.

"Using Eclipse gives them more opportunity to attract 3GL Eclipse developers. It makes OpenEdge's abilities more attractive to those folks," Hammond added.

Betty Zakheim, director of product marketing at Progress, boasted that OpenEdge is the first integrated platform that can be used to develop and deploy service-oriented architecture applications. Zakheim contrasted OpenEdge and its proprietary ABL language with Java EE, a 3GL programming environment that requires a separate development environment. "The developers and deployment team get the burden of making sure it all works together. OpenEdge is less complex," said Zakheim.

Hammond agreed with Zakheim's assessment—with one caveat. "3GL users can switch vendors," said Hammond. "The devil's bargain with 4GL is that you get a lot of productivity, but you get trapped into that vendor's environment. It is a trap, if the vendor cannot extend [it]." ∎

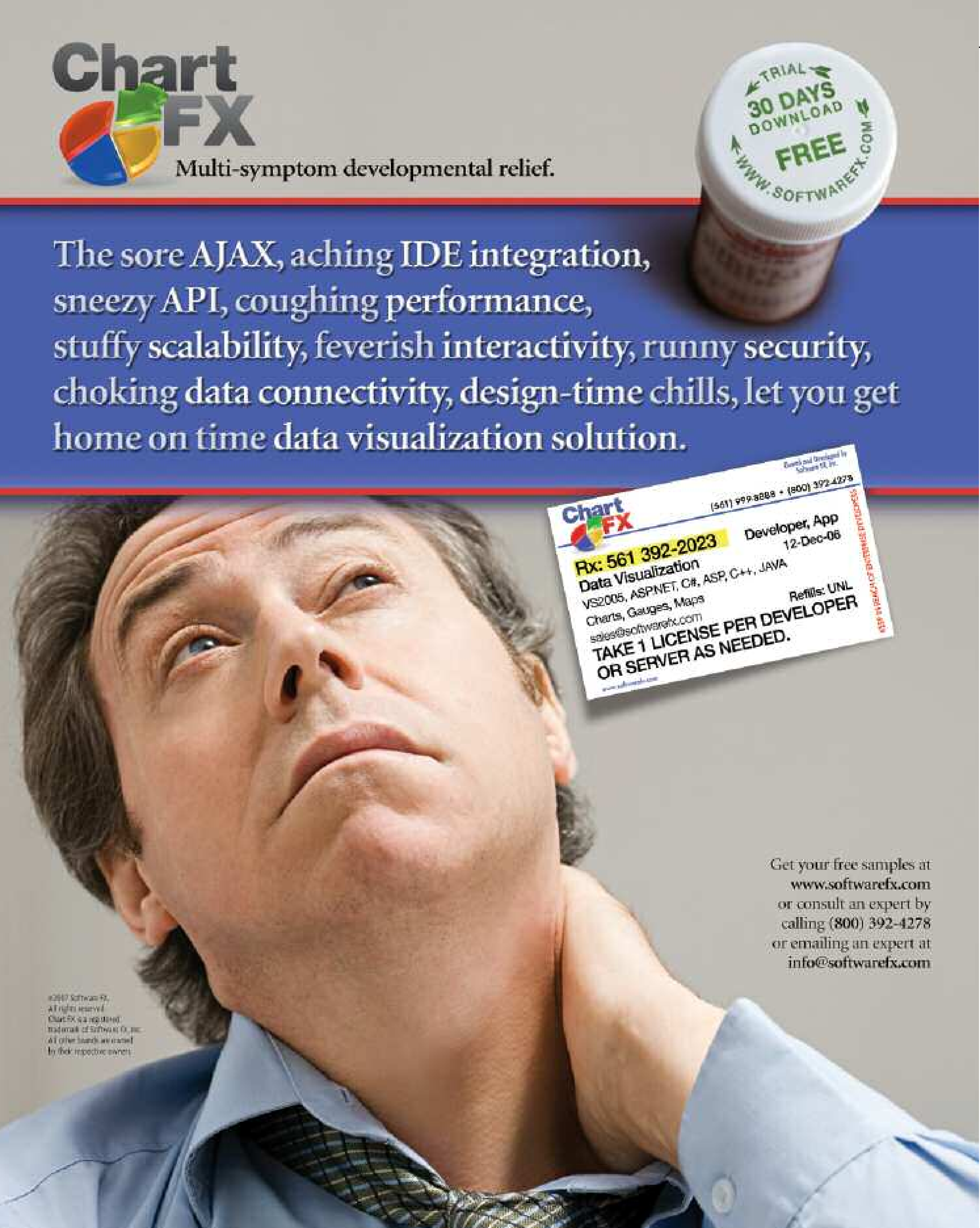


Chart FX
Multi-symptom developmental relief.
TRIAL
30 DAYS
DOWNLOAD
FREE
WWW.SOFTWAREFX.COM
The sore AJAX, aching IDE integration,
sneezy API, coughing performance,
stuffy scalability, feverish interactivity, runny security,
choking data connectivity, design-time chills, let you get
home on time data visualization solution.
Chart FX
(561) 999-8888 • (800) 392-4278
Developer, App
12-Dec-06
Rx: 561 392-2023
Data Visualization
VS2005, ASP.NET, C#, ASP, C++, JAVA
Charts, Gauges, Maps
Refills: UNL
sales@softwarefx.com
TAKE 1 LICENSE PER DEVELOPER
OR SERVER AS NEEDED.
Get your free samples at
www.softwarefx.com
or consult an expert by
calling (800) 392-4278
or emailing an expert at
info@softwarefx.com
©2007 Software FX.
All rights reserved.
Chart FX is a registered
trademark of Software FX, Inc.
All other brands are owned
by their respective owners.

U.S. Requiring Software Security Enhancements

Mandate might put onus for hardened installations on contractors

BY ALEX HANDY

Windows Vista has presented the U.S. military with an opportunity to push some of its security burdens back onto Microsoft. Late last year, the armed forces, National Security Agency and a handful of other government agencies joined with Microsoft to define a securely configured form of Windows Vista, the first time such collaboration has taken place.

While the NSA has previously developed so-called "security-enhanced" forms of operating systems, this move marks the first time that an operating system's creator has been in on the process. The practice may soon change how contractors are able to sell their tools to government agencies.

Alan Paller, director of research at the SANS Institute, a Bethesda, Md.-based cooperative research and education organization, spoke at the RSA Conference in San Francisco in February about the coming shift in how government agencies handle security. Paller should know; he has testified before Congress about computer security numerous times. Paller said that the beginnings of this shift have already arrived in the form of this securely configured version of Windows Vista.

"Right now, the vendors deliver systems that make users go through all sorts of hoops to harden their systems after installation," said Paller. "Why? Because people would whine if users couldn't use a feature because of security. The practice is to simply leave every door and window unlocked by default. But what if the purchaser said, 'We like your product, but we want it configured securely?'" While many operating systems are available in secure forms, Paller said that much of the system-hardening required by the military is done by government IT workers after an initial installation.

It doesn't cost Microsoft any more money to securely configure Vista, says SANS Institute's Paller.

And that is what the military and its constituent agencies did. Former U.S. Air Force CIO John Gilligan first began a crusade to fix the Air Force's IT woes in 2001, according to Paller. Now, six years later, Microsoft will soon be forced to lock all those doors on government-issued editions of Windows Vista. In his RSA presentation, Paller quoted Gilligan on his reasons for moving in this direction: "It costs us more to clean up after Windows compromises than to buy the software in the first place. This will have to change."

Gilligan began his new initiative by eliminating third-party Windows vendors from the Air Force's contractor pool, Paller said, adding that as a predominantly Windows shop, the Air Force now purchases its operating system licenses directly from Microsoft. In addition, all applications purchased by the Air Force will have to be tested and certified to work on this "safe" version of Windows Vista, placing the security and reliability onus firmly on the contractors' heads. Paller said that he expects other agencies to follow the military's example as the year moves on.

FISMA MIASMA

This shift in government requirements, which Paller predicted would materialize sometime in 2007, might signal a shift in how federal agencies handle IT security, said Paller. He cited numerous examples of rising international and espionage threats while also pointing out the problems inherent in the Federal Information Security Management Act (FISMA) of 2002.

First among the problems with this law, Paller argued, is what he categorized as a poor series of metrics used to measure the effectiveness of the security in place at government agencies, that he claimed focus more on checklists than performance. "We have to stop blaming the users," said Paller. "What we measure right now is: Do you have a plan for immediate response to security issues? What if you have a plan and you're not executing the plan? Doesn't matter: As long as you have a plan, you get an A."

Paller also claimed that FISMA measures the number of employees that have taken a security awareness class, but does not measure actual systemic compliance with the policies advocated in such a class. But he discussed the possibility of change, especially in the metrics imposed by FISMA. Paller observed that government security officers are beginning to understand the shortcomings of FISMA, and may soon overhaul the requirements and systems in a manner similar to those recently undertaken by the military.

"We can get leverage on this problem by getting the vendors to help us," said Paller. "Does it cost Microsoft any more money to securely configure Vista? No." But simply pushing configuration issues onto the vendor can save thousands of man-hours for government IT workers, he added. ▮

RSA: CHATTING ABOUT SECURITY

The RSA Conference and Expo in February brought together some of the best minds in software security. We wandered the show floor, popping questions to some of the bigger brains in attendance. Here are some comments we found interesting:

"The only reason why cross-site scripting [XSS] is so popular is it's a single attack you can look at and name. Most hacks and most ways of breaking in aren't really done, in my mind, via XSS and SQL injection. They're done through a series of mistakes in the application logic during development. And you can't give a name for that. It's human error, and it's something that will never end."

—Caleb Sima, CTO and co-founder, SPI Dynamics

"If you look at the spending over the course of the last three to five years, you're going to see a lot of people spending money to perimeterize their security, and not a lot of focus on the applications themselves. You don't think of this as something you're gonna solve by writing new software that's more secure. When I worked at HP in 1992 writing DCE components, I was worried about time services. I could have cared less about security. I was jamming, I was getting the code done, and it was out there and functional. I never expected these different applications that I'd written to be used in the ways they were. You can't tell me that someone doing chat architecture in 1975 knew that those services would be exposed in an SOA architecture in 2007."

—Jack Danahy, CTO, Ounce Labs

"Any organized crime group that isn't using these techniques should be sued for malpractice."

—Patrick Morrissey, U.S. Secret Service, discussing cybercrime

"There's definitely a real problem out there. For most people, the problem doesn't exist until they experience it themselves. Look at all the private data consumers want protected; some people are doing a pretty poor job of securing that data. The problem everyone has raised, from a vendor perspective, is that this is an unsolvable problem. That's why we really need to be much more prescriptive in what we're trying to solve from a business perspective, not just a tech perspective."

—Kurt Roemer, CSO, application networking group, Citrix Systems

ALM Providers Embrace Security

◂ continued from page 5

cation security message intentionally. "What [the announced Gauntlet partners] have in common is that all of them do static analysis."

Infusing analysis into the ALM tool set and the ALM process is what Gauntlet is all about, said Borland's Cheng. Many ALM tools are integrated with application security offerings, but such integrations are typically point to point, he said. For instance, Cenzic Hailstorm is integrated with Hewlett-Packard's testing tools, formerly Mercury. And Fortify SCA works with the Rational Software Development Platform. But Gauntlet, when used in tandem with Borland LQM offerings, can bring together data from many different tools, generating reports on key security trends, for instance. "You could see that code checked in by this group of developers resulted in a rise of this particular type of vulnerability," said Cheng, offering an example. (Forrester's Schwaber noted that reports that pull data from many different products can also be created with Microsoft's Visual Studio Team System.)

Ovum's Rotibi said Borland is taking a much deeper look at some of the individual phases in the ALM process, and application security is a part of that. That approach is "quite canny," she said. "They have solved their problem around CodeGear," she said, referring to Borland's recent spin-off of the developer tools group. "They have nothing to lose, and they are going for it in a big way." ▮

Reticulitermes Hesperus, or Subterranean Termite—unchecked, property damage estimated at $3 billion per year.
Electron Micrograph, 140X

McCabe Shows Off IQ in Three Ways

New editions of quality tools deepen code review and collaborative capabilities

BY DAVID WORTHINGTON

The IQ product line from quality management vendor McCabe Software is not just for QA test teams anymore; new editions throw developers into the mix. Last month, McCabe released an overhaul of its McCabe IQ product line, now structured as a hierarchy of developer, team and enterprise editions.

Each product includes metrics that evaluate the complexity and quality of applications. The team and enterprise editions have added functionality to convey pertinent project information among team members and management.

All McCabe IQ products support numerous programming languages, including Assembler, C, C++, COBOL, Java and the .NET languages. As a whole, the product facilitates code review and refactoring legacy applications. Dale Brenneman, vice president of software quality solutions, claimed that many customers purchase McCabe software just to understand how undocumented legacy applications work.

DEVELOPERS EDITION

McCabe IQ Developers Edition is designed to help programming managers make decisions about suitable development paths and how to allocate resources. IQ maps application architecture, provides a data dictionary, compares modules and flags complex code. The module comparison, change analysis and data dictionary are new to this version.

After processes are run, information about source code logic is visualized with structure charts, object-oriented class diagrams, and flow graphs of modules. A data dictionary is also produced. The company claims that no other tool available does this type of visualization.

IQ also evaluates software quality. Brenneman explained that the process is not monolithic; the logic and data in the source code predicates what metrics are used. Up to 125 different metrics comb through lines of code to assess software application quality.

"It takes an incredible amount of intelligence to look at source code and calculate these sets of metrics," Brenneman noted. "We are not just obtaining numbers that exist in the code. IQ software examines all classes, modules and their relationships."

MIDDLE AND HIGH END

The midtier McCabe IQ Test Team Edition is a new offering that keeps tabs on which modules of an application have been tested and which have not. It tracks and analyzes code that has a defined data set and locates redundant code.

At the top end, McCabe's IQ Enterprise Edition incorporates the other feature sets and provides new high-end features such as enterprise reporting and secured online test data collection. ▮

Jean David Ichbiah, Ada Lead Designer, Dies at 66

BY P. J. CONNOLLY

Pioneering computer scientist Jean David Ichbiah died on Jan. 26, reportedly of complications from a brain tumor and a recent fall. He was 66.

Ichbiah was considered the chief designer of the Ada programming language, which had its roots in his prior work on systems implementation languages.

In 1975, Ichbiah was a member of CII Honeywell Bull's programming research division in Louveciennes, France, when the U.S. Department of Defense (DoD) realized that, of its vast stable of embedded programming languages, none supported safe modular programming, and many were either hardware-dependent or obsolete. The DoD's Higher Order Language Working Group spent the next few years creating a series of working papers that culminated in the "Steelman" requirements document of 1978.

Photo by K.N. King

Ichbiah (shown in a 1993 photo) was at CII Honeywell Bull when the DoD chose his team's language proposal.

Because no programming language of the day met the "Steelman" criteria by including now-common features such as exception handling, parallel computing and run-time error-checking, the DoD hired four teams to design a language that would meet or exceed the specifications. Ichbiah's team, code-named Green, submitted the proposal that was officially adopted in 1979 and given the name Ada, after Lord Byron's daughter, Augusta Ada, Countess of Lovelace.

IBM fellow Grady Booch was a recent graduate of the Air Force Academy when he was assigned to what would become the government's Ada Joint Program Office (AJPO), in the midst of what he called the "bakeoff" between Green and the other proposals.

Booch noted that Ichbiah's contributions shaped the evolution of software development: "You can honestly say that the work in Ada, and the work that Jean did…were the catalysts to the work I did on object-oriented design."

Ichbiah was a brilliant man, said Booch, "and had such a deep understanding about language design, and the ideas of strong typing and abstract data types that, back then, were relatively new concepts. But he was able to…put in his head all of these ideas and weave them together, to produce what was at the time quite a beautiful language. Jean was way ahead of his time."

The first standard Ada version was adopted in 1983, and was kept under strict control by the DoD. But in 1987, Ada 83 was adopted as an ISO standard and released to the public. Within three years, more than 200 validated Ada compilers were in use.

Meanwhile, Ichbiah had left CII Honeywell Bull to found Alsys (now Aonix) in 1980, which continued the work of defining Ada and eventually entered the compiler business. He later moved to Massachusetts to take a more direct role in the management of the company's U.S. subsidiary.

After leaving Alsys, Ichbiah started Textware in 1992, which specialized in text entry hardware and software for mobile devices. At Textware, he continued his practice of awarding fine wine as a contest prize: Ichbiah had presented a bottle of Beaujolais to the only person who found a semantic error in the draft specification of Ada, while in recent years, Textware's winning entrants were presented with bottles of Dom Perignon.

Ichbiah was named a member of the French Academy of Sciences in 1987, and was a knight of the country's Légion d'honneur. He was interred in Wakefield, Mass., near his home of Burlington. ▮

HPC PIONEER KEN KENNEDY DIES

BY P. J. CONNOLLY

Ken Kennedy, founder of the Rice University computer science department and groundbreaker in the field of high-performance parallel computing, died in Houston on Feb. 7. Complications from pancreatic cancer caused his death, according to a university spokesperson.

Kennedy was director of the university's Center for High Performance Software Research, and co-chair of the President's Information Technology Advisory Committee from 1997 to 1999, but continued to teach undergraduate courses even after his recognition as an expert in his field. ▮

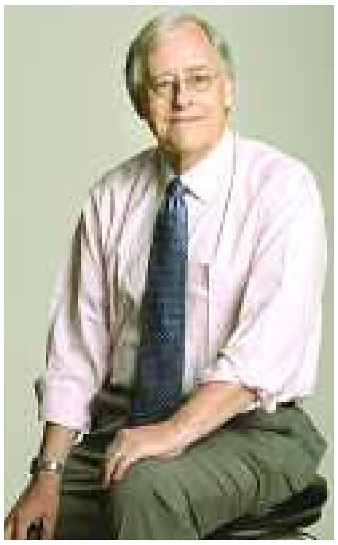
Chaos Made a Name for Standish

Report's influence remains strong 12 years after first publication

BY DAVID RUBINSTEIN

Ed Yourdon remembers the impact The Standish Group made with its first Chaos Report, published in 1994. He also remembers wondering who these guys were.

"It made a big splash at the time," said Yourdon, author of "Death March," the quintessential book on project failure. "But it was not the only set of statistics. We had never heard of The Standish Group; I believe it's one guy up in Massachusetts. There were other, more prominent people—Capers Jones, in particular, and Howard Rubin—running around at software engineering conferences presenting similar numbers."



Death march projects are back, says author Ed Yourdon. 'Everyone wants to be YouTube.'

Suddenly, there was another credible source saying the same things the others were saying, but the Chaos Report was the one embraced by analysts and software providers, to show how important it was to buy and use their tools.

The 1994 Chaos Report "has had a remarkable lifetime," Yourdon added. Working as an expert witness in court cases brought when projects fail, he said he continues to hear those early success-rate numbers bandied about. "But now, the counterattack is that it's a 12-year-old report."

While Yourdon agrees with the reasons cited for more project success—better development managers, iterative development and the growth of the Web infrastructure—he offered one more of his own. "The end users, or stakeholders, are more mature and experienced. They've been burned a few times, and won't sign on for a project that will take years to complete," Yourdon said.

The fact that the 2006 Chaos Report shows only incremental improvement in software quality does not surprise Yourdon.

"If the demands of the market had remained stable, we could have gotten better," he said. "But we're still asked to do more and more under competitive pressure, when the requirements remain difficult."

As for death march projects, Yourdon reported that they, too, are on the rise after having fallen off for a while.

He traces the history of the death march to the beginning of the dot-com era, when teams of developers would work on huge, and hugely exciting, projects knowing that if they succeeded, they could become billionaires. Then came the Y2K death march projects, which were not as much fun to work on.

From then until recently, Yourdon noted, people "were pretty much licking their wounds." But now, death march projects "are back with a vengeance. Everyone wants to be YouTube." ∎

Standish: Less Chaos in Development

◂ continued from page 1

ment, iterative development and the emerging Web infrastructure.

"There is better project management expertise and technique," he noted. "Managers have a better understanding of the dynamics of a project." Iterative development, Johnson said, makes it easier for people to get what they want. "Part of the education process [for iterative development] is that people are better able to articulate what they want out of a project."

Finally, Johnson added that the emergence of the Web "plays a fairly significant role. The idea that you can get things out quickly and people can learn it, touch it and give feedback creates a more dynamic experience."

The 2006 report also shows what Johnson called a stunning improvement in the metric used to measure project value. If the assets of a failed project can all be considered waste, in 2006, software value was measured at 59 cents on the dollar. In 1998, that figure was 25 cents on the dollar. "You can look at that as a 24 percent compound average growth rate since 1998," Johnson said.

The 1994 report can be read at The Standish Group Web site (www.standishgroup.com); the 2006 report is still being completed. ∎

New RAP Hits to Debut at EclipseCon

BY ALEX HANDY

Call in the ATF, because Eclipse is going to RAP.

At March's EclipseCon in Santa Clara, the Eclipse Foundation will release new milestones of the AJAX Tools Framework and the Rich AJAX Platform, dubbed ATF and RAP, respectively. While neither will be in a final form, both projects will offer new features that should bring enterprises the level of tooling they've come to expect for Java.

Mike Milinkovich, executive director of the Eclipse Foundation, said that RAP gives Java developers a window into this wild, new AJAX world. "The idea," said Milinkovich, "is to leverage the existing tools and the existing skills from RCP and make those available to the AJAX developer."

Thus, RAP allows developers to build their applications in Java, resplendent with Java-specific XML and database libraries. Once the application is complete, RAP can deploy the functionality in AJAX.

RAP is not yet a completed project, however. EclipseCon will mark the first major publicly discussed release of RAP, according to Milinkovich.

Also on the docket for EclipseCon 2007 is a beta release of Eclipse ATF. This is a more traditional Eclipse tool, said Milinkovich. "The interesting thing about ATF is that it hasn't hit 1.0 release yet, but already a lot of companies are building on top of it," he said.

ATF includes the debugging and development tools that programmers expect with Java. But here, the specifics are all targeted at the needs of AJAX development: ATF offers direct XML and DOM inspection tools, syntax highlighting and code validation.

"The really cool thing about ATF is the profiling in the debugger," said Milinkovich. "You can watch the packets go back and forth. You can inspect the XML that's being sent back and forth. The other thing that's cool is that it's hooked up to the Firefox debugging and DOM tools."

At the present time, ATF supports only the Mozilla Firefox Web browser; however, Milinkovich said that the project may soon offer Internet Explorer support, now that IE 7 has cleaned up some incompatibilities with JavaScript. But for now, the EclipseCon release of ATF will add support for Mac OS X to the mix. ∎

eclipseCON 2007

CONFERENCE: March 5–8
Santa Clara Convention Center

TUTORIALS:
Monday, 8:00 am–6:00 pm

TECHNICAL SESSIONS:
Tuesday, 10:00 am–5:00 pm
Wednesday, 10:00 am–5:30 pm
Thursday, 10:00 am–3:30 pm

EXHIBIT HOURS:
Tuesday, 9:30 am–1:30 pm; 2:15 pm–8:00 pm
Wednesday, 9:30 am–2:45 pm

KEYNOTE SPEAKERS:
Tuesday, 9:00 am–10:00 am, Scott Adams
Wednesday, 9:00 am–10:00 am, Robert Leftkowitz
Thursday, 9:00 am–10:00 am, Herbert Thompson

ECLIPSE COMMUNITY SPOTLIGHT:
Thursday, 3:30 pm–4:30 pm, panel moderated by Mike Milinkovich, Eclipse Foundation executive director

www.eclipsecon.org

ILOG JRules Adapted for Business Analysts

BY DAVID WORTHINGTON

ILOG is betting that it has simplified its JRules 6.5 business rule management system to the point where impact analysis and discerning business logic can be done by non-developers.

JRules 6.5 allows the expression of business rules as decision services in a service-oriented architecture. Coding is not required, and according to ILOG product marketing director Henry Bowers, the resulting decision services are "transparent" because the business logic is "in a language everyone can understand—[even those] outside of the black box."

Bowers continued, "Business analysts need to understand what logic is implemented, which policies are applied, where it fits in the business level, and how it fits into business process orchestration."

The look-and-feel of JRules Rule Team Server is now customizable using CSS, while Rule Studio now supports Eclipse 3.2. Rule Scenario Manager has usability enhancements to input and output data structured in business model terms, accepts input from multiple instances of Microsoft's Excel, and organizes testing artifacts by rules set in the Rule Scenario Manager console and Rule Studio. ▮

ETL Goes Open Source

BY P. J. CONNOLLY

As IT systems become more diverse, tools that provide extract, transform and load functionality become necessary for data consistency and usability. What its developer calls the world's first open-source ETL product became available a month ago, when JasperSoft added JasperETL to its lineup of business intelligence (BI) products.

JasperETL includes a graphical ETL process editor, the Job Designer, which provides functional process views to business analysts. Another tool, the Transformation Editor, graphically maps data transformations and allows editing of complex mappings and transformations. A debugger provides real-time tracking of ETL statistics, while a fourth tool maps out the BI workflow.

JasperETL supports more than 30 different data sources, including the usual suspects of flat and XML files, and leading databases. POP and FTP servers can also supply data to a BI process via JasperETL. A number of configuration wizards assist users in assimilating complex file formats and metadata.

The so-called open source edition of JasperETL is available now for free download and use from the JasperForge.org community Web site. A professional edition that adds a shared repository for metadata use in a team environment is expected in the spring.

The new ETL product was developed as part of a partnership with data integration tool vendor Talend, which provided the necessary expertise. ▮


Register by March 16 Save $200!
Software security training is a great idea.
Now there is a conference to teach us what we need to know.
April 16-17, 2007 | San Mateo Marriott
San Mateo, CA
San Francisco Bay Area Location!
Attend the Next
SOFTWARE SECURITY SUMMIT
A BZ Media Event
Diamond Sponsor
FORTIFY SOFTWARE
Gold Sponsor
Mu Security
Media and Industry Sponsors
SD Times
Software Test & Performance
hakin9
queue
CoDe
HSToday
Learn How to Build Secure Software
Test the Security of Your Software
Understand Software Security Vulnerabilities
Implement a Layered Approach to Application Security
Architect Security Into the Development Life Cycle
www.S-3con.com
For sponsorship or exhibiting information, contact David Karp at dkarp@bzmedia.com or 631-421-4158 x102.

Liberty Alliance Suffers an Identity Crisis

◂ continued from page 1

CTO of identity management at HP Software. "I don't think the adoption was slowed down because it didn't work; it was just a market education project."

But that market is clamoring for identity solutions: At this year's RSA Conference, a noticeable number of vendors were offering new solutions to identity problems. The Liberty Alliance, however, must fight to make its solutions known, said Roger Sullivan, Liberty Alliance management board president and vice president of identity management at Oracle.

Among the alliance's goals for 2007 is to collaborate with existing and new identity projects.

"You've got OpenID, the Identity Commons, [and the Eclipse-based] Project Higgins.... There's a reason those things are going on," said Rouault. "They're trying to fill a niche in the market that they think that Liberty doesn't solve. It might be the case that Liberty doesn't solve it, or it does and they don't know. We want to sit down with them and talk about what we're both doing that is synergistic."

"One of the things I've seen at some conferences I attend is people trying to address problems that Liberty solved three years ago," said Sullivan. "Shame on us for not making that information available."

That's why the alliance will begin a concerted push for more openness in 2007, said Sullivan. This move has been heralded by the creation of openLiberty.org, a project designed to build a repository of open source examples of Liberty Federation standards implementations. The project's Web site was opened in January, and will serve as a code resource for developers.

"Identity management can be somewhat daunting for folks who want to roll their own solutions and who have not done it before," Sullivan said. "I think that open source implementations of Liberty specifications can play a vital role in filling that need."

STARS VERSUS LIBERTY

Complicating the task of the Liberty Alliance has been the confusion around Web services and the overlap between the alliance's work and WS-* specifications, said Rouault. "The WS-* set of specifications are, in essence, plumbing for Web services. The Liberty work in Web services is really about the efficient profiling of how you do identity-based Web services in a secure manner," he said. "In some cases where specifications don't exist, then we add that into the [WS-*] framework. They're not two separate stacks at this point, though they might get positioned that way."

Said Sullivan: "We think that WS-* is going to be a force as it moves into the open standard industry. There needs to be a bridge between those two industries. We think there's a valid role we can fill that needs to be done.... Customers need to deploy both [WS-* and open Web services standards]. If they don't deploy both, they will most certainly be working with customers who use both." ∎

ESRI Maps Out GIS Platform for SOA

Connects spatial analysis tools with app dev framework, Web services

BY DAVID WORTHINGTON

Feeling lost? A Geospatial Information System (GIS) can point you in the right direction. It displays, edits and queries geographically referenced information that then is made available through mapping, spatial analysis and modeling functions. GIS applications are multipurposed and versatile, providing scientists, historians, marketers and criminologists alike with useful information to examine locations and assets.

ESRI is charting a new direction for GIS by integrating its applications into a service-oriented architecture (SOA). ESRI has taken its existing spatial design tools and coupled them with an application development framework (ADF) for .NET and Java. The new ArcGIS 9.2 uses a combination of Web services protocols and administrative tools to achieve SOA support. The end result is that GIS services are connected with enterprise services.

ESRI provides three of its own development platforms: ArcGIS Desktop; ArcGIS Engine for building custom GIS applications; and ArcGIS Server, which offers a centralized repository for ArcGIS Desktop and a portal for GIS applications.

These platforms allow the use of four common development platforms. Cross-platform C++ and COM are supported in addition to Java and .NET.

The ArcGIS framework supports JavaServer Faces-based Web controls and templates, which are exposed in the IDE as drag-and-drop elements for JavaServer Pages. Enterprise JavaBeans are included for mapping, geocoding, geoprocessing and network analysis tasks. Web and enterprise service templates are also available.

CONTROLS, COMMANDS FOR VS

If Java is not brewing at an organization, Microsoft's .NET 2.0 platform is another option for visually developing ArcGIS applications. Templates, wizards, code snippets, documentation and component-level help are integrated into the Visual Studio IDE through a plug-in. ArcGIS offers nearly 200 custom controls and commands for Visual Studio 2005.

"Generally speaking, everyone is moving to SOA," said Yankee Group analyst Laura DiDio. "It is a new way of doing business, and support for this is designed to cause the least amount of disruption to the existing software, hardware and Internet working infrastructure, while at the same time, providing customers with expanded services and functionally." ∎

OpenMake Wants to Be Known as the Build Meister

Company changes name, shifts focus to developers with new release of build solutions

BY JEFF FEINMAN

Not many companies change their name as often as this year's Super Bowl half-time performer Prince, who has appeared under such different guises as "The Artist Formerly Known as Prince" and an unpronounceable symbol. But it's not at all unusual for a company to rename itself after the flagship product, which is what happened in February when Catalyst Systems re-entered the build management market as OpenMake Software.

The renaming announcement came not with electric guitars or flashing lights, but with a timeline for updates to the company's tools: Mojo 7.0, a free build process management tool, is slated for general availability on March 5; and Meister 7.0, the company's larger, long-term build solution that replaces OpenMake 6.41.1, is set for an April 1 release.

Tracy Ragan, COO of OpenMake, said the product line until now "catered substantially to the configuration management administrator. What Meister is going to do, is hand off some of that control back to the developers. The new product will be built on the Eclipse Rich Client Platform, so the whole user interface will be more developer-centric than it has been in the past."

NEW…AND NOT SO NEW

The most important feature of Meister 7.0, Ragan said, is the new Eclipse RCP front end, which has a more "standardized" look-and-feel for developers. As a result, the ability to manage or customize build services will be simplified, she said. Meister will retain many features from previous OpenMake releases, including minimized script redundancy and automatic code refactoring.

Meanwhile, Mojo 7.0, will be available through the company's Web site (www.openmake.com). The offering gives developers ad hoc script management, build metrics, and shared build and release process management. It is aimed toward smaller developers, who can eventually upgrade to Meister 7.0 or Meister for Java, which provides knowledge base services for building Java JAR files.

Ragan confirmed that the company changed its name from Catalyst to OpenMake because the product had such strong brand recognition among customers.

Stephen King—no relation to the author—the new CEO of OpenMake, said the company's upcoming product releases offer a tremendous growth opportunity. "Our product is sold by companies like Serena Software, Borland and MKS, and we need to address the rest of the market by putting out our own sales force," he said. "Offering a free version of the product will go a long way toward building our user base." ∎

OSGi Alliance, JCP at Odds on Component Support

◂ continued from page 1

integral to the progress of JSR 291 since its creation in February 2006. He described JSR 291 as an effort "to define how OSGi [the model for an in-virtual-memory SOA for networked systems] as a component model will work in the context of Java SE."

Specifically, Colson said, the OSGi Alliance has solved a problem that's plagued Java for years, and now the alliance is seeking JCP validation of its solution.

"In Java today," said Colson, "it's sort of a one-application environment. You start a JVM, and you run an application with it, then you tear down the JVM. What OSGi does is enable you to run multiple services on top of the same JVM at the same time, each with independent life cycles. There is a strict model for import and export, with a well-defined versioning system for those components. If 'A' depends on 'B' and 'C' is independent, I can run those all on the same JVM. I can manage their life cycles independently. I can update 'C' without disrupting 'A' and 'B.' I can also disrupt the 'B' element without disrupting 'A.'"

'NOT A BAD SPEC'

But Hani Suleiman, CTO of financial technology solutions provider Formicary and a member of the executive committee that voted on JSR 291's public review in January, said that the work OSGi has done doesn't need to be validated by the JCP.

"It's not that it's a bad specification," said Suleiman, who, along with Sun, voted against the continuation of JSR 291. "I don't think that the JCP should be used to get a JSR number. I don't see the benefit." Despite these two nay votes, the specification passed its public review and continues on its way to final ratification.

Colson said the benefits of running OSGi's component model through the JCP are obvious: More eyes mean more input. While Suleiman's objections were based around the specification's lack of work within the JCP, Colson said the JCP's review of OSGi's work will result in some changes to the overall project.

"OSGi is now on release 4," said Colson. "With the [successful completion] of JSR 291, there will be a 4.1 release." That release, he said, will incorporate the suggestions and input offered by members of the JCP.

Colson pointed to JSR 232, a completed specification that brought OSGi's work onto the Java ME platform. That spec, said Colson, was created through a combination of work inside and outside of the JCP, in a manner similar to that of JSR 291.

Said Mike Milinkovich, executive director of the Eclipse Foundation: "We're going to start seeing Eclipse technology show up in runtimes in the Java ME space. I think OSGi is the first component [model] that started in the ME space and has grown rapidly into the enterprise." The Eclipse runtime is largely based on OSGi's work.

But for Suleiman and Sun, the words of IBM and other OSGi members have not assuaged their fears that JSR 291 risks pushing the JCP closer to becoming a validation organization, like Ecma or OASIS.

"I was told that this is in fact a rubber-stamping effort and that the OSGi spec will not change," said Suleiman. ∎

HackerSafe Security Claims Questioned

◂ continued from page 1

cannot, of course, actually guarantee that. Napa, Calif.-based ScanAlert, which was founded in 2001, guarantees that the sites that bear its mark meet minimum standards established by organizations such as the Payment Card Industry (PCI) consortium, which mandates, among other things, that Web sites are scanned for vulnerabilities at least quarterly, said ScanAlert CEO Ken Leonard [see sidebar].

To earn the HackerSafe seal, a Web site must engage ScanAlert's services, subject itself to daily, remote audits of its Web site and resolve any detected problems within 72 hours, he said. "Seventy-five percent of the sites scanned fail initially, but over time that number goes down." Failure to fix a problem within the specified time period results in automatic, electronic removal of the certification mark, he said.

One aspect of the scan is concerned with network security. But to earn the seal, a Web application is also subjected to black-box testing, sometimes called penetration testing. This approach simulates Web site attacks, looking for known flaws, such as SQL injections, that a hacker could exploit to steal key data. "The biggest opportunity to improve security is at the application level," said Leonard.

The company also offers source code analysis services, using its own proprietary source code analyzer. But that service, where customers submit source code to ScanAlert's lab, is not required to earn the HackerSafe certification mark, he said.

PAYING FOR CERTIFICATION?

ScanAlert's services range from US$400 to $100,000 per year. Asked how a company that sells security offerings can position itself as a third-party, independent certifying authority, Leonard reiterated that 75 percent of the sites tested fail, and said: "We are an independent third party. We certify the security of our customers, and the certification mark is controlled by us."

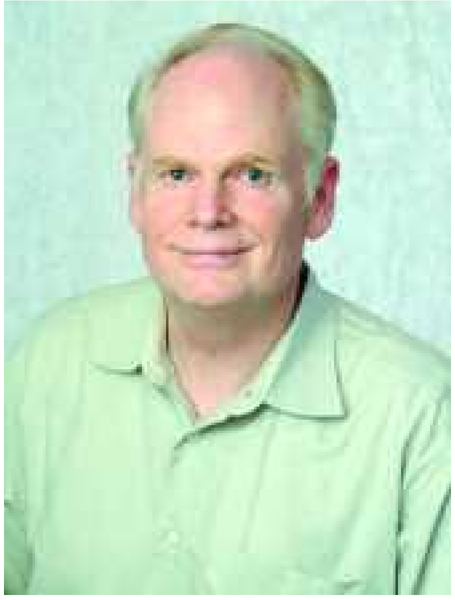
Fortify's Thornton had a different take. "ScanAlert charges you money to say you are compliant," he said. That, he said, is "a total discredit to the consumer and to the companies who are serious about security."

Caleb Sima agreed. "The [certification mark] bothers me," said the chief technology officer of SPI Dynamics, which sells black-box testing and source code analysis tools. Online shoppers get a false sense of security when they purchase from Web sites that bear the HackerSafe seal, he said. And, among members of the security industry, there is a widespread perception that customers who buy ScanAlert's services do so not to improve security, but to use the logo on their Web sites. "That is the talk you hear at [security] conferences."

But it doesn't matter what the motivation is, said analyst Robin Bloor, who heads Bloor Research. "It's incredibly smart to put the HackerSafe logo on the Web page." Customers may buy ScanAlert's services to boost sales, but they are still getting the benefit of daily security scans. And for many companies, that is more than they were doing before, he said. "Most companies don't do the level of security checking they should."

Boosting sales is what the HackerSafe certification mark is all about, said Leonard. The company positions its offerings to senior sales and marketing executives. It is difficult to sell security services to developers and IT professionals, he said. "But if you talk to the marketing side of the organization, they sit up and listen."

That was true for Lynnette Montgomery, general manager of e-commerce for Levenger, a retailer that sells pens, paper and desk accessories. The company is currently working with ScanAlert to certify www.levenger.com. "We didn't have a security sign for the Web site," she said. "I made reference calls to ScanAlert customers, and every retailer I talked to received a conversion rate, some as high as 20 percent. Our goal is to build the brand and increase the conversion rate."



Sites that display the HackerSafe seal garner more sales, claims ScanAlert CEO Ken Leonard.

Asked whether Levenger was conducting security tests on its Web site prior to engaging ScanAlert, and whether it is using the company's source code analysis services, Montgomery said no.

According to ScanAlert, more than 70,000 Web sites bear the HackerSafe certification mark, including those operated by Ace Hardware, Blue Nile, Home Depot, Linens 'n Things, Logitech, National Geographic, PETCO, PetSmart, Sports Authority and Vermont Teddy Bear. "There are more sales from sites with HackerSafe," claimed Leonard.

When asked if a Web site bearing the HackerSafe seal has ever been attacked, Leonard did not answer directly. "The HackerSafe certification greatly reduces that likelihood," he said, but added that if an attack should occur, the certification minimizes liability. "It demonstrates you were exercising [security measures] compliant with the PCI standard."

Comprehensive application security requires an ongoing set of best practices throughout the application life cycle, said Fortify's Thornton. Conducting daily Web vulnerability scans, such as those offered by ScanAlert, is better than doing nothing, he said. "If you took away the extortion angle, it would be awesome." ▮

PCI: The Standard for Credit Data Safety

BY JENNIFER DEJONG

In September 2006, American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa International jointly announced the formation of the PCI Security Standards Council.

Made up of companies that issue credit cards, the council was established to manage ongoing evolution of the PCI standard, earlier managed informally. The council's mission is to improve payment account security by fostering broad adoption of the PCI Data Security Standard. The standard specifies processes and precautions for handling, processing, storing and transmitting credit card data across all payment channels, including retail stores, mail order and e-commerce.

Released in September 2006, PCI Data Security Standard 1.1 outlines 12 broad-based requirements, grouped under six categories. Many address network security and access control issues. But requirement 11—to regularly test security systems and processes—also deals with application security concerns.

It specifies, among other things, that Web applications are subjected to quarterly vulnerability scans performed by an outside vendor qualified by PCI. (ScanAlert is one such vendor; Qualys is another.) Requirement 11 also mandates application-layer penetration tests at least once a year, and after any significant application or modification.

Failure to meet the PCI Data Security Standard 1.1 by June 2007 could result in a fine as high as US$500,000, and could also bar a business from processing credit card transactions. Penalties can vary from one credit card company to another. ▮

A 12-STEP PROGRAM

The requirements, outlined in depth at www.pcisecuritystandards.org, are as follows:

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

Requirement 3: Protect stored cardholder data.

Requirement 4: Encrypt transmission of cardholder data across open, public networks.

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software.

Requirement 6: Develop and maintain secure systems and applications.

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know.

Requirement 8: Assign a unique ID to each person with computer access.

Requirement 9: Restrict physical access to cardholder data.

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data.

Requirement 11: Regularly test security systems and processes.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security.

Sources: www.pcisecuritystandards.org, www.qualys.com

—Jennifer deJong

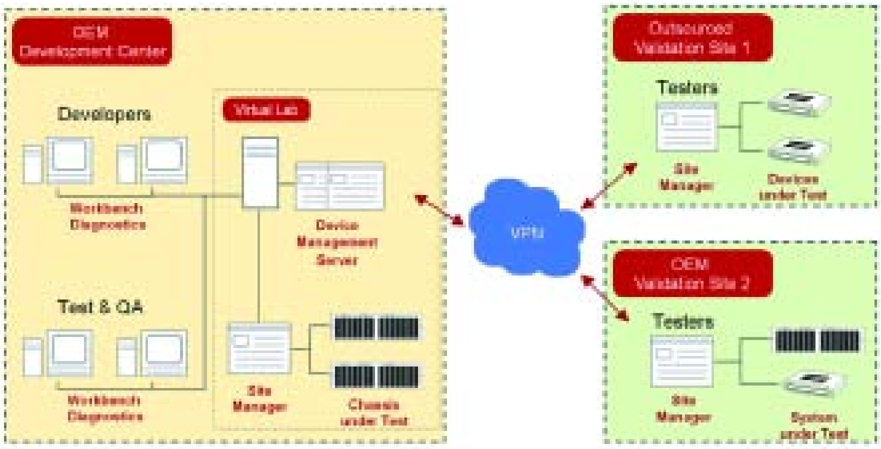
Wind River Rolls Out Diagnostics Package

BY P. J. CONNOLLY

Wind River Systems released a new software diagnostics package in February designed to simplify embedded device development, by allowing cross-functional teams to collaboratively engage in debugging, quality assurance and testing.

Wind River Lab Diagnostics works with the company's VxWorks 6.x on most PowerPC and Intel processors, VxWorks 5.5.1 on PowerPC, and Wind River Linux 1.4 on PowerPC and Intel.

Lab Diagnostics is Wind River's latest device management offering, following last year's release of Wind River Field Diagnostics. The two can work in tandem, to provide a complete and coherent approach to embedded software development and deployment. The twofold advantage of this process is that developers and test teams are working with actual devices instead of black boxes as early as possible in the development cycle, while troubleshooting can take place without modifying the source code or restarting the device.



Source: Wind River Systems

Wind River Lab Diagnostics developers work with a number of QA and validation teams, capturing device information locally and transmitting it securely to a central server for analysis.

Paul Henderson, vice president of business development for Wind River, explained that the new Lab Diagnostics package was designed "to wring problems out of devices and get products to market [more quickly]."

He continued, "Strategically, we've been extending our focus from the development phase of the life cycle, to…test, validation and manufacturing, as well as products for deployment support."

The heart of Lab Diagnostics is the Device Management Server, which provides a central repository for test tools and their results. This repository can be a MySQL or Oracle database running on top of a JBoss or WebLogic application server, which in turn can be a Linux, Solaris or Windows machine.

But Workbench Diagnostics is where the real action takes place. Building on the Eclipse-based Wind River Workbench, it's a root-cause analysis tool that allows developers to add so-called sensorpoints to the device under test. Sensorpoints are used to add diagnostic instrumentation to live applications without modifying the underlying code or device. Sensorpoints can be maintained in a test-specific catalog on the management server, refreshing the Site Managers as necessary. Workbench Diagnostics also collects core images of system memory and allows developers to stress running software with fault injection as part of the test plan.

The Site Manager application collects the data from the in-house lab and outside testing and validation facilities; this is similar to the deployment of Field Diagnostics, except that in the field, the testers and validators are actual customers. The data from the various Site Managers is rolled up to the Device Management Server, allowing consolidated analysis against authorized, known data. Site Manager is designed to work in firewalled environments and offers VPN support for secure communications. ∎

Putting POSIX in People's Pockets

Feature Pack for S60 adds new C++ and Java APIs

BY P. J. CONNOLLY

Nokia in February announced plans to introduce an update for the S60 platform later this spring: The S60 3rd Edition Feature Pack 2 includes enhancements in software architecture and usability, and is aimed at midmarket devices.

The new features include support for instant playback while downloading media and animated call notification, to thrill end users; support for the demand paging of virtual memory is included to thrill developers.

Feature Pack 2 marks the debut of Open C, an extension of the POSIX libraries for Symbian OS, as a native feature; previous iterations of S60 3rd Edition are supported through a plug-in. The libraries reduce the amount of Symbian-specific C++ coding for developers by providing function implementations from nine libraries: libc, libcrypt, libcrypto, libdl, libglib, libm, libpthread, libssl and libz.

Ravi Belwal, senior technology expert at Forum Nokia, explained that "implementation of Open C will allow the developer community to reuse software assets, thereby increasing their productivity. Because C libraries are commonly used to create applications on other platforms, Open C support significantly simplifies the process of porting an existing application to the S60 platform."

The new Feature Pack offers a number of API enhancements in both the C++ and Java categories. The Java updates focus on improving support for the Mobile Service Architecture subset of JSR 248. These include new versions of the Scalable 2D Vector Graphics API for J2ME (JSR 226), the Java Bluetooth APIs (JSR 82), and the Mobile Information Device Profile (JSR 118).

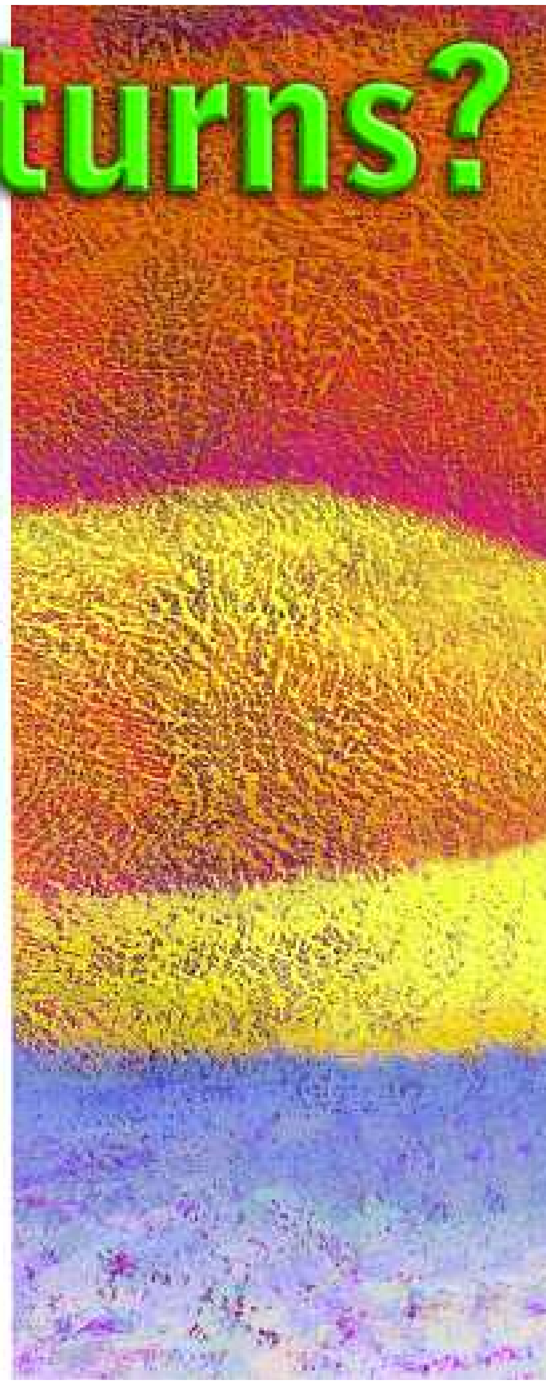
The improvements in the C++ APIs introduce a new feature for S60 developers, Application Interworking (AIW), which allows the embedding of functionality from one application into another. The AIW Dial Service Consumer API and a new Map and Navigation AIW API are the first APIs that Nokia is releasing in this category.

Three other map framework APIs are part of the new Feature Pack, enabling applications to consume geocoding, mapping and other navigation services.

Seamless application-level network roaming is a must for building the next generation of mobile apps. Feature Pack 2 adds two APIs to help manage network connections: One handles the user interface while the other exposes connection settings.

The new Feature Pack also supports two new user-side APIs in the S60 environment. A "middle softkey" API enables that feature on supported handsets, while a status pane API provides users with an at-a-glimpse view of the device's situation.

In addition, Feature Pack 2 offers an updated version of Adobe's Flash Lite as an optional component. Flash Lite 2.1 allows users to perform inline editing, and to use metadata and XML sockets in their multimedia. ∎



Many Happy Returns?

Different measures of SOA success make finding real ROI a difficult job

BY GEOFF KOCH

GalaxyPlus Credit Union Systems got its first taste of service-oriented architecture in 2005. That was when the 200-person division of Fiserv, based in Troy, Mich., set out to expose its core account and loan creation offerings as services. What followed was a tale with several tried-and-true SOA themes.

The GalaxyPlus IT team was hobbled by a legacy, mainframe-based system; a database that was capable only of accepting precompiled SQL statements written in PL1 and C; and tool sets that did not support SOA-mandatory XML. Given contractual obligations and competition in the market, the company could neither charge its customers for the infrastructure upgrade nor ask these customers to migrate from their own mostly IBM/AIX-based platforms.

The solution was one part do-it-yourself hand-coding and one part vendor-assist. GalaxyPlus programmers wrote their own JDBC driver to get around their database issues and then selected an open-source Java EE application server, JBoss, to host the application.

REACHING NEW MARKETS

Compared with the option of building a new application from scratch, bolting on a new Java- and open source-based service to the old system helped to save on development time and infrastructure costs. But the real payoff, said GalaxyPlus IT development manager Dan Carnell, was the ability to access new markets. Today, GalaxyPlus' new account and loan creation services are integrated into CRM applications used by credit unions, thus making it easier for credit union call centers to sell new loans or accounts to their members.

"The services we created spawned an entirely new product line," said Carnell, a 17-year industry veteran who previously worked as director of application programming at Quicken Loans. "This group now brings in significant revenue for GalaxyPlus.

"Our goal now is simple—to build flexible solutions to service not just our 300 clients, but thousands of diverse credit unions," he continued. "That's a powerful way to examine our return on investment—the sky's the limit."

That, for better or worse, is a pretty good encapsulation of the thinking about return on investment, or ROI, associated with SOA projects today.

Most vendors and early adopters agree that the easiest SOA benefits to measure include reduced IT and development costs and faster time-to-market. However, the same crowd seems to find any discussion of these benefits to be downright boring. Instead, like Carnell, many reserve their most enthusiastic language for promises of a paradigm shift in IT that points directly to new customers, markets and profits.

The problem is that few reliable rules of thumb exist even for doing a rough calculation of any projected SOA benefits, industry-changing or otherwise. But there are ways to "guesstimate."

'GUESSTIMATING' ROI

One approach borrows heavily from the world of business process optimization, which involves the sometimes tedious work of scouring workflows for inefficiencies and then religiously monitoring the workflows with a variety of scorecards. Another option is to assign numerical values to attributes such as complexity of systems, services and processes and then do the math to come up with the relative value of various SOA choices. A third way is to compile the growing number of survey results about expected SOA payoffs in various business categories, then use the accumulated wisdom of the crowd as a measuring stick for one's own SOA efforts. A fourth tack that's unfortunately consistent with the ignominious tradition in IT of trafficking in FUD—fear, uncertainty and doubt—is to talk about the perils of being carried along by the SOA wave only to drown in costs associated with managing a growing and unruly stable of services.

Most of these methods carry the whiff of quantitative respectability, though many interviewed for this article said that, for the time being, attempts at measuring SOA ROI yield only highly subjective and very rough approximations of true value.

"There's always a huge fudge factor in terms of just how you account for all the intangible assets and costs," said Bill Hayduk, founder and president of IT services organization RTTS in New York City. "So much of the ROI calculation depends on the person doing the calculating."

C IS FOR COST

Still, SOA advocates are not going to be let off the hook anytime soon when it comes to pitching new projects that have some grounding in business and financial realities, especially given who's on the receiving end of the pitches. More than 50 percent of respondents in BEA Systems' November 2006 "SOA Cost Benefit Survey" said that top executives—the CIO (22 percent), CTO (18 percent) or CFO (12 percent)—were the primary SOA sponsors within their organizations.

C-level approval for big IT endeavors is nothing new. But it may be a mistake, at least according to BEA, to use a traditional IT yardstick for measuring the potential value of a services-based approach. In a July 2006 Exec2Exec newsletter, the company pointed out that typical IT projects affect just one line of business and a limited set of business processes. In contrast, the tentacles of a SOA project often reach throughout an organization.

Help desks may receive fewer calls due to proactive governance and monitoring. Developers may see their productivity increase as they move to a more incremental approach to coding. System architects may benefit from having a strong, extensible foundation for future projects. And by exposing SOA interfaces to customers and business partners, a company conceivably can shore up existing value chains and even, à la GalaxyPlus, reach new markets.

These and other SOA claims too often sound breathless. One way to do a sanity check is to steal best practices from business process optimization, another discipline that looks out broadly on a business's day-to-day landscape. In a Sept. 16, 2006, Web seminar sponsored by Sun Microsystems, titled "ROI of SOA," Pradipa Karbhari gave a thorough account of how to first build a business case and then measure the impact of a SOA implementation.

Karbhari, national director of Web services and SOA at Milwaukee-based technology consultant SilverTrain, emphasized the importance of thoroughly cataloging mundane business operations and their many subtle inefficiencies. Are electronic orders somehow being delayed in the entry phase? Are the preferred customers getting the right discounts? How accurate is the shipping date promised to the customers?

Understanding the answers to questions like these is one way to estimate the potential value of a SOA project, Karbhari said in her presentation. The answers also can be used to build scorecards that attempt to show cause-and-effect relationships between subterranean changes to IT plumbing and bigger-picture business objectives.

Say the goal for next quarter is to grow overall revenue by 20 percent. Hitting this target, in Karbhari's example, depends in part on increasing online sales, which in turn might be nudged along by improvements to customers' online experience when it comes to order entry, discounts and ship dates.

This kind of operational forensics work is tedious, and many a hotshot

technologist has quietly groaned when the operations wizard expert stopped by for a visit, clipboard in hand. Yet these same methodologies seem to point the way to a respectable set of SOA ROI estimates—though Karbhari admitted the set is incomplete.

"The challenge is that the architecture itself doesn't offer a quantifiable means for organizations to calculate a return," she said. "Instead, the architecture needs to be considered in the larger context of business process optimization and business agility and as more of a long-term investment."

DO THE MATH

A career coder might blanch at the prospect of inventorying his employer's many workflows and instead prefer the model suggested by David Linthicum, a SOA consultant based in Reston, Va. Linthicum, a former associate professor of computer science and a prolific author, advocates an approach that limits its analysis to the more familiar confines of IT.

In a November 2006 article, titled "Determining the ROI of Your SOA," Linthicum outlines a straightforward, quantitative model based on two of the most enticing SOA promises—saving money by reusing services and making money by quickly adapting to new business conditions.

The value of reusing services, according to Linthicum's paper, depends on at least three variables—the number of services that are reusable, the complexity of services and the degree of reuse from system to system. A system composed of 100 potentially reusable services with an overall degree of reuse of 50 percent and an average services complexity of roughly 300 function points has an overall value of 15,000 function points (100 services x 0.50 x 300 function points per service).

According to Linthicum, most firms know roughly what they're paying per function point, an ISO-recognized metric to express the amount of business functionality an information system provides to a user. So his simple equation is one way of measuring gross value from a SOA deployment. The final step, subtracting implementation costs, gives the net value of the system.

Using a different set of three variables—the degree of change over time, the ability to adapt to change and the relative value of change—a similar equation can be used to assign a dollar value to the increased agility that comes with SOA. Here, however, the margin for error starts to feel uncomfortably large. How, for instance, do you assign a specific value to the ability to adapt to change?

"Determining…SOA's ROI is not an exact science," Linthicum wrote in his concluding paragraph. "[B]ut with some analysis and some realistic data points, you can figure out how much value your SOA implementation has brought you, or will bring you."

SURVEY SAYS

Insecurity runs deep in IT, and no matter how thorough a company's self-assessment of a given technology strategy is, even the smartest managers eventually start looking for validation in the market at large. When it comes to SOA, what these managers will see is a raft of surveys about the expected value from an all-services, all-the-time approach.

Unfortunately, several of these surveys spring from vendor-sponsored research that, like it or not, is a fixture in the technology industry. BEA's aforementioned SOA Cost Benefit Survey—a survey of North American and European companies with annual revenues greater than US$1 billion conducted by GCR Custom Research—indicated that 40 percent of firms expected to spend $1 million or more on SOA efforts during the next 12 months, a shockingly high number especially since the same survey reports most of these companies are currently engaged in only two or three SOA projects.

"A million dollars for a couple of SOA projects—wow," wrote Joe McKendrick, SOA research consultant and ZDNet contributing editor, in a November blog posting. "That seems kind of high, and beyond the reach of most organizations. I don't think most managers can go to management requesting a million dollars for a few SOA projects."

Broadly speaking, however, the BEA survey is consistent with other, more independent market research. For example, companies in the BEA survey

continued on page 36 ▸

Measuring Real Value of SOA a Tough Job

◂ continued from page 35

said they expect their SOA deployments to trim integration costs by 18 percent and maintenance costs by 20 percent. A July 2006 survey by AMR research found similar savings in initial costs (20 percent) and total-cost-of-ownership (22 percent), categories roughly analogous to the two used in the BEA survey.

Compared with the BEA survey, the AMR research was based on a much broader and deeper sample. More than 1,000 people, 651 of whom were using or considering SOA projects, completed Web-based surveys. Respondents were split roughly evenly between the United States, Europe and Asia and came from manufacturing, retail, telecom, banking and other industries. Nearly half of those in the SOA sample came from companies with annual revenues of less than $100 million.

Among the other expected tangible improvements from SOA in the AMR results:

- Increase ROI by 22 percent.
- Improve employee productivity by 27 percent.
- Reduce errors by 28 percent.
- Increase users of the services-enabled application by 22 percent.
- Shorten time to receive measurable value to the business by eight months.
- Decrease implementation times by eight months.

These and other survey results from many market research firms—Forrester Research plans to apply its Total Economic Impact model to SOA later this year—suggest another passable way to decide whether a SOA project is worth it. Namely, if the implementation won't result in payoffs in line with industry norms, it probably is not.

FUD AND OTHER FUNNY BUSINESS

Yet another way to think about ROI comes from the flip side of the mostly sunny attributes spelled out in SOA-related market research and marketing material. This darker line of thinking, which predictably warns against the wait-and-see approach, holds that nothing can hold back the rise of loosely coupled services and that, ready or not, SOA is set to sweep into nearly every IT organization. Businesses that have plans to manage and govern this inevitable bloom of services, many of which will spring from users who may be savvy about business problems but naive in the ways of IT, will succeed. Those that don't will fail.

Of course this is FUD at its finest, invariably doled out generously by vendors or consulting firms that stand to make a buck from SOA-branded software or professional services. However, at least one analyst said it's probably not prudent to completely ignore the warning.

"Enabling certain business users to manage and evolve business processes without direct IT involvement is one of the most ambitious of SOA goals, and for good reason—such a vision requires bulletproof governance as well as mature tooling that's only now beginning to reach the market," wrote ZapThink senior analyst Jason Bloomberg in a January 2007 ZapFlash research note.

Beyond the nod to governance, Bloomberg's comments hint at another trend in SOA analysis that, aside from providing another way to think about ROI, may have profound implications for in-house technologists of all stripes. Namely, SOA seems to be simultaneously eroding and elevating the place of IT in business.

Asked about SOA ROI, Bob Eve, vice president of marketing at SOA data services firm Composite Software, wrote that one measure of success in a recent SOA-based portal project was that "IT operations didn't need to get involved." Through its media representative, Serena Software wrote that SOA, "by creating clear and concise definitions of business applications and associated bills of material," should make it easier to move IT tasks offshore.

Is this the further marginalization and commoditization of technology? Perhaps. But in anecdotes like these, Iona Software CTO Eric Newcomer also sees a surge of SOA-inspired efforts by companies to finally reconcile their IT spending with their overall business objectives.

"Up to this point in time, IT has been much more focused on automating previously manual activities, and the ROI was easier to calculate," said Newcomer. "Now that the majority of manual tasks has been automated, corporations are starting to take a look back, rationalize what they've done and align spending with corporate instead of departmental goals."

What's most surprising is that it's the services-focused approach itself that seems to hold the key to evaluating IT as more than a cost sink and instead as a bona fide means to reach new markets and customers.

"Without something like SOA in place," said Newcomer, "it is difficult, if not impossible, to measure IT investment relative to its impact on top-line revenue."

So to measure the return on investment from SOA, it sounds like you first have to implement…well…SOA. ∎

FROM THE EDITORS

Where Freshness Counts

SD Times was given a sneak peek at the 2006 Chaos Report, which shows that enterprise software developers are doing a better job of building software than they were back in 1994, the year the first groundbreaking Chaos Report was released by The Standish Group.

While a special report exploring the 2006 data isn't expected to be completed until April, we were told that more projects end in success, and fewer in outright failure, than was the case 13 years ago. This shows, among other things, that organizations are taking development as a professional discipline more seriously.

When asked for comment, analysts and other industry watchers expressed amazement: "Hey, it's about time they updated that old report." That's what we initially thought, too—but were then surprised to learn that the Chaos Report is updated frequently. It's just that nobody talked about the new numbers.

The 2006 Chaos Report is actually the sixth that The Standish Group has published; the first came out, as mentioned above, in 1994, and then has been updated every two years since 1998. The first report took on a life of its own, as its gloomy statistics about product failures were embraced and widely distributed by software tools makers, many of whom sold silver bullets to address those projects.

Standish chairman Jim Johnson even pointed out that some vendors made the numbers appear even worse, lumping "challenged" projects with "failed" projects to paint an even more dire picture of the state of professional software development.

When the Chaos Report numbers showed improved project successes in the late 1990s, those newer reports didn't play as well in the tools makers' marketing departments. That's why those tools makers continued to distribute the 1994 version of the report.

But now, a new breed of vendor can sell off the new numbers. Johnson says that among the reasons that software quality is improving, iterative development and better project management are often cited—so now tools makers working in those areas have some new ammunition.

The truth, according to Standish, is that failures are down and successes are up. If a software tools maker tries to get you to buy based on the 1994 Chaos Report figures, now you know why.

Old Software Bugs Never Die

While February's RSA Conference offered plenty of reason to check in on the state of secure coding, another February event triggered further thought on the matter. Solaris 10 and the unfinished Solaris 11 were both found to contain a nasty exploit that allows anyone logging in over telnet to take over root, simply by appending "-f" to the front of the log-in.

What's so terrible about this exploit is not its power, nor its simplicity, but the simple fact that not one software solution available on the RSA expo floor would have caught this bug. Programming tools can't find flaws that are actually boneheaded features. And few QA people are well versed enough in penetration testing to kick open the screen doors developers may have substituted for sturdier barriers.

The solution? Systematic and methodical peer code review. While agile techniques would have helped, that sort of religious war isn't necessary here. What is needed is teamwork and a lot of time spent looking over other people's code—perhaps the most thankless and difficult task a programmer can perform.

It's the dirty little secret of the security industry: Programmers are always under deadline, and hackers aren't. The programmer's job is not to prevent the hacker from breaking the software: The task at hand is to raise the bar so that only a well-versed hacker can break the software.

Unfortunately for Solaris users, the bar for this latest exploit was exceptionally low. With so many low-set bars, it shouldn't be too tough to significantly improve the security of your applications with a weeklong pizza-and-code review party at the office. ∎

Security As A Requirements Issue

Software development organizations are never going to produce truly secure applications until they understand that security is not something you can begin worrying about ad hoc, after the application is written. The common response to securing applications has been to attempt to identify and remove all of the application's security vulnerabilities at the end of the development process. However, this bug-finding approach is not only resource-intensive, but also largely ineffective.

Adam Kolawa

PATHS TO DISASTER

In fact, such an approach could lead to a disaster because testing can never find all of the security vulnerabilities that might be in a piece of software. Why? Finding errors is an NP-complete problem, which means there are always an infinite number of paths through the application. You can't guarantee that all those paths are free of vulnerabilities because it's simply not feasible to identify them all and then test each and every one of them for every possible vulnerability.

Penetration testing is really inefficient at finding errors. What penetration testing does is try to create conditions under which an error can be discovered. This is very difficult. It needs to find the right paths to hit potential vulnerabilities, and then determine if the vulnerabilities can actually occur. This will find some errors—but is unlikely to expose all of them.

Scanning the code with static analysis security tools can also find some vulnerabilities. However, even data flow analysis, which is commonly recognized as the most sophisticated breed of static analysis, has its limits. Since only a limited number of steps are followed, some paths or path segments will be overlooked. Moreover, today's applications lack an obvious starting point because they are data-driven and event-driven. Finding and following all paths through such applications is difficult. As with penetration testing, some problems might be exposed, but others will certainly be overlooked.

A more practical way to ensure that software is free of security vulnerabilities is to approach security from the perspective of requirements. The application behaving in a way that does not reveal confidential information or allow unauthorized actions is just as critical as its ability to provide new features or to enhance the scope of existing ones, so the application's security requirements should receive the same consideration and treatment as its functional ones.

Granted, it is possible to prevent some common security vulnerabilities if you take a general approach to security rather than treat it as a requirements issue. A requirements-based approach is not needed to prevent common vulnerabilities such as SQL injection, parameter manipulation, buffer overflows, cross-site scripting and so on.

However, the dangerous new breed of application attacks exploit application logic that was not designed with security in mind, so the only feasible way to prevent them is to consider security as a requirements issue, in the context of the specific application you are building.

For example, consider the recent attack where a retail application storing unnecessary credit card details permitted credit card counterfeiting. Or, the attack where the application gave many user accounts search privileges inappropriate for their roles; attackers managed to access accounts that had these excessive search privileges and use these accounts to potentially access hundreds of thousands of "confidential" personal records.

Running common security tests on such applications would have done nothing to stop such attacks. Preventing them would have required someone to have considered the potential for exploits, then define functional security requirements that made such exploits impossible.

For instance, let's return to the attacks where the application gave many user accounts search privileges inappropriate for their roles, These attacks could have been prevented with functional security requirements that users in a class expected to access tens of records per year could only access tens of records per year—not thousands.

Defining, implementing and verifying functional security requirements really is the industry's most powerful weapon against attacks on application security.

USING REQUIREMENTS APPROACH

So, how does a software development organization go about treating security as a requirements issue? First, someone needs to determine the security requirements and define them in a security policy. If the organization has designated security experts, they should be writing these requirements. If not, security consultants could be brought in to help develop appropriate requirements for the specific application under development. Obviously, this would require considerable interaction with the internal team members most familiar with the application.

Next, the development team needs to

implement these security requirements as they write the code. Since most developers admittedly know little about security, it's important to teach them about development practices for building secure software and show them how to apply those practices to their code so they can maintain it.

As soon as each security requirement is implemented, the development team should start verifying that it's implemented correctly—just as they would verify any other requirement that they implemented. Many security requirements can be verified through custom static analysis rules. Others might require unit testing, component testing or other techniques. In any case, at least one test case should be created for each requirement, and every test created should be added to the regression test suite, which should be run automatically every 24 hours to ensure that code modifications and additions did not "break" or otherwise impact the previously verified security functionality.

In addition to verifying security requirements at the unit level, developers should be responsible for using static analysis tools to ensure that the code they write is free of common security vulnerabilities such as unvalidated inputs. As I mentioned earlier, this general automated code analysis is not, on its own, sufficient to guarantee security. However, since it's such an easy way to eliminate some vulnerabilities, it would be a shame to ignore this low-hanging fruit.

Later, when the application can be exercised realistically (for example, when a Web interface is available for a Web application or Web service), penetration testing can be used to validate that the functionality is operating correctly at the application level. Although penetration testing is not an effective way to uncover the bugs in an application that was developed without heed for security, it is a very effective way to perform "positive tests" that can validate that attempted penetrations do not succeed.

Security needs to be built into the product from the earliest phases of development, with the support of a well-defined team workflow and an automated infrastructure.

Human intelligence is required the first time that a complex task is performed, but automation can typically be leveraged to repeat the task from that point forward. This frees team resources for the more complex and creative tasks that can't be automated—such as anticipating additional vulnerabilities in the application logic, designing requirements that prevent them, figuring out how to implement those requirements in the code, and designing tests to validate that they are indeed safeguarding security as expected. ▮

Adam Kolawa is chairman and CEO of Parasoft, which sells software testing products.

LETTERS TO THE EDITOR

Standards as Politics?

On the article "Enterprise Architects of the World Unite" by David Rubinstein [Feb. 15, page 10], I have a question: Is this going to be another exercise in forcing people to use SQL/Relational models, or is it actually going to be about enterprise architecture?

As a data architect—I was the only speaker on the subject at the IBM IOD conference in 2006—and a business consultant (22 years' experience), I've seen a lot of standards and testing that only solidify the position of some subset of the existing models. Is this standards as politics? I'm just hoping that Open in this case means inclusive.

Charles Barouch

DRM NIGHTMARE

A standing ovation [for Zeichick's Take, "Digital Rights Mis-Management," in the Feb. 8 News on Thursday newsletter]!

DRM does not serve consumers' needs, and indeed treats them as criminals, more often than not.

Ray Blaak

Like you, I have an extensive CD collection ripped to MP3. However, there is one music download service I use—emusic—precisely because it imposes no DRM. The selection is heavily skewed toward indie/alternative, but that suits me fine. Cheers!

Pat Patterson

WHAT DO YOU THINK?

SD Times welcomes feedback. Letters should include the writer's name, company affiliation and contact information. Letters become the property of BZ Media and may be edited for space and style. Send your thoughts to feedback@bzmedia.com.

The worldwide software revenue for information access with search is projected to nearly double between 2006 and 2011, according to a recent report from Gartner. Gartner uses "information access" to cover a range of disciplines, including content analytics, information presentation and taxonomy creation and management.

The calculations in "Dataquest Insight: Forecast for Information Access with Search Technology in the Enterprise, 2006-2011" include new licenses, subscriptions, updates and upgrades, as well as hosting, maintenance and technical support.

SD Times
SOFTWARE DEVELOPMENT
The Industry Newspaper for Software Development Managers

Software Development Times
Issue No. 169
March 1, 2007

Editorial

Editor-in-Chief
David Rubinstein
+1-631-421-4158 x105
drubinstein@bzmedia.com

Managing Editor
Patricia Sarica
psarica@bzmedia.com

Senior Editors
P.J. Connolly
pjconnolly@bzmedia.com
Jennifer deJong
jdejong@bzmedia.com
Alex Handy
ahandy@bzmedia.com

Associate Editor
David Worthington
dworthington@bzmedia.com

Assistant Editor
Jeff Feinman
jfeinman@bzmedia.com

Columnists
Andrew Binstock
Larry O'Brien

Contributing Writers
Mary Jo Foley
Geoff Koch
Susan Messenheimer
Lisa L. Morgan
Carol Weiszmann

Editorial Director
Alan Zeichick
+1-650-359-4763
alan@bzmedia.com

Art & Production

Art Director
Mara Leonardi

Art/Production Assistant
Erin Broadhurst

Sales & Marketing

Publisher
Ted Bahr
+1-631-421-4158 x101
ted@bzmedia.com

Southwest U.S./Asia
Robin Nakamura
+1-408-445-8154
rnakamura@bzmedia.com

Northwest U.S./Canada
Paula F. Miller
+1-925-831-3803
pmiller@bzmedia.com

Southeast U.S./Europe
Jonathan Sawyer
+1-603-924-4489
jsawyer@bzmedia.com

Northeast/Central U.S./Canada
David Lyman
+1-978-465-2351
dlyman@bzmedia.com

Advertising Traffic
Phyllis Oakes
+1-631-421-4158 x115
poakes@bzmedia.com

Marketing Manager
Marilyn Daly
+1-631-421-4158 x118
mdaly@bzmedia.com

List Services
Nyla Moshlak
+1-631-421-4158 x124
nmoshlak@bzmedia.com

Reprints
Lisa Abelson
+1-516-379-7097
labelson@bzmedia.com

Accounting
Viena Isaray
+1-631-421-4158 x110
visaray@bzmedia.com

Reader Service

Director of Circulation
Agnes Vanek
+1-631-421-4158 x111
avanek@bzmedia.com

Customer Service/Subscriptions
+1-847-763-9692
sdtimes@halldata.com

BZ Media

President
Ted Bahr

Executive Vice President
Alan Zeichick

BZ Media LLC
7 High Street, Suite 407
Huntington, NY 11743
+1-631-421-4158
fax +1-631-421-4045
www.bzmedia.com • info@bzmedia.com

BPA

Logging: Think Before You Write

The other day, I was in the middle of a wide-ranging comparative product review. One product—a high-priced IDE sold by a major software vendor that spends considerably on teaching developers how to write better software—refused to install. The installer was written in Java and repeatedly filled my screen with a stack trace resulting from a null pointer reference. As you might expect, I got on the wire and was eventually put in touch with the developer who wrote the installer. He asked me several questions, made me run MD5 checksums on the product's binaries, and finally asked me to send him the installation log to see what he could find.

Before sending off the logs, I decided to examine them myself. Alas, I found the usual kind of log entries that are almost completely without value. It was a series of XML records that logged the date and the time and a short phrase describing the current step in the installation process. You know, entries such as "performing initialize phase" and "performing install phase." It did flag the problem and noted the elapsed time and the diagnostic "java.lang.NullPointerException." This content is characteristic of much of the logged data you find in the detritus that package installers leave in their wake.

Unfortunately, it is all the wrong information. As you might reckon, even the fellow who wrote the code could gather nothing from this log. All he could tell was in what step of the process the blowup occurred. And the diagnostic value of that is not zero, but close to.

There is an expression that has become a refrain in unit-testing circles: Every software failure indicates a missing unit test. This is true in general, and undeniably so in this case—a null pointer error in an installer strongly suggests a missed unit test. But the real problem here is that the logging was done with no real thought as to its purpose: The central purpose of logging is diagnostic. So developers need to log information that is useful for debugging, rather than the nearly useless recital of elapsed time for steps.

The key question here is: What data to record? And the answer should be viewed in the context of what the unit test to fix this problem would need. In my opinion, installers have two responsibilities that must be exhaustively tested: identification of the capabilities of systems on which the installation will take place, and validation of the options the user chooses. Tellingly, neither of these items was captured in the log. Not a word about the system configuration, and not a peep about which features I chose to install. So, then, how could the engineer use the logs to identify or reproduce the problem? He couldn't. So, then, why bother logging? And, of course, without the minimal level of information about configuration and choices, there's no chance of writing a unit test to cover the problem.

Logging is a universal programming activity. There are at least three established logging packages in Java (Java SE, logj, Commons logging). Most major languages have several logging options as well. It's also the defining use case for aspect-oriented programming. And yet there is virtually no discussion about what to log. Go into Amazon and enter "Java logging," and you'll find a handful of books that mostly talk about the travails of configuring log4j. Unfortunately, configuring a logger is the easy part. It distracts programmers from thinking about what should be logged.

But even the programming aspect, if you insist, is seriously incomplete. Try some time to find how to unit-test a logger that writes to the console. (So far, I've found this topic covered in just one book—Jeff Langr's excellent "Agile Java.") In many ways, I think, developers see logging as a "nice to have" feature, so they view any logging effort they make as sufficient, even admirable. This is far from the case. Logging needs to be thought out just as carefully as any other diagnostic part of programming.

Returning to the case at hand: Logging single line events with an abbreviated description and a time stamp is a reasonable (although not great) approach when you're logging transactions in a really busy Java EE server. Logging has to happen fast, and you are mostly diagnosing transactions that did not complete successfully, rather than finding root causes. However, most programs—such as this software installer—have no time pressure or resource constraints that prevent detailed capture of diagnostic information. And in those many cases, logging should be planned with far more care than is common today. ▮

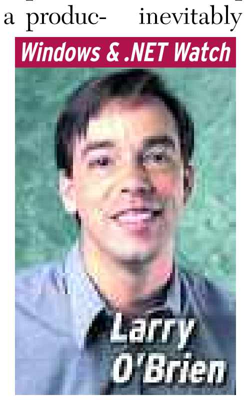
Andrew Binstock is the principal analyst at Pacific Data Works. Read his blog at binstock.blogspot.com.

The Problem With Estimation

A puzzle, according to national security writer Gregory Trevertin, is a conundrum that has a concrete answer, albeit one that is presently unknown to you. Programmers love puzzles (How do I create this visual effect? How do I collate the data from disparate sources?) and excel at solving them. Mysteries, though, are questions that no one could answer, even if all current information were available (Is ASP.NET the very best choice for delivering my next application?). Less-experienced developers don't like mysteries very much and spend a great deal of time trying to convince themselves and their peers that mysteries can be reclassified as puzzles. Then, in the course of every career, comes the realization that every true difficulty in software development has a human, not technological, basis. And humans, for better or worse, are inherently mysterious.

This realization (which could be called "The Weinberg Epiphany," after Gerald Weinberg and his seminal work on the psychology of computer programming) is an important milestone. Fledgling team leaders or managers abandon the hope of discovering the undocumented APIs to develop perfect requirements, awesomely productive teams and blissfully precise customers. Instead they realize that their jobs are going to center around issues of communication and persuasion, egos and emotions, frustrations and unexpected personal crises. They've realized the difference between "software development" and "programming" and, hopefully, the difference doesn't discourage them.

Sometimes, though, things get out of hand. Happy programmers are productive programmers; therefore, a productive environment is one in which programmers have fun. Bring video game consoles and foosball tables into the work environment.



In the dot-com days, I worked for a company that was going to spend some $10,000 and several hundred square feet to build a sensory deprivation tank (perhaps as a place to get away from the sound of the foosball table). The video game industry, in particular, takes misplaced pride in uncontrolled projects, boasting that their products "will ship when they're ready," and shrugging off yearly death marches to hit the crucial holiday season (the "Post Mortem" features in Game Developer magazine are always entertaining, although often in a "can't look away from the horror" way).

Not long ago on a private mailing list, a noted writer said of software project estimation: "I've seen so much time wasted on an activity which provides so little real value that I'm a bit jaded on the entire subject. Frankly, I struggle to see how you would need anything more than a 20-page white paper on this topic." This is taking the mysterious too far. While it's true that the final cost and ultimate ship date of an application are inevitably dependent on adjustments and decisions made during the course of development, the business world is filled with people who very reasonably value clear accounts of what can and cannot be accomplished over the course of multiple quarters. Often, they reasonably prefer to avoid the expense and furor of incremental deployment and value honest assessments of a long development process more than the self-reported productivity increases that often accompany loosening of formal procedures.

Of course, one of the great problems with older processes for controlling large development projects is that teams often report "on track" development for the first 90 percent of the system, and then that last 10 percent takes as much effort as the first. Such overruns are problems, though, not mysteries; they can be addressed with pervasive binary quality gates (automated test suites at both the unit and system level), risk-driven development priorities, and project estimates developed using disciplined techniques, not those created by stacking up all the "that seems like a couple days' work" assurances and measuring the height of the pile.

Software estimation techniques are like the C programming language. They work, but they demand diligence and precision. You don't expect a novice to write a defect-free data structure the first time out of the gate, and you shouldn't expect the best-case and worst-case scenarios of a newcomer to be anywhere near the mark. Accurate estimates are possible, but not in a few hours.

According to Steve McConnell's excellent recent book "Software Estimation: Demystifying the Black Art," (a title that triggered the theme of this column), sophisticated estimation techniques can lead to accuracies of plus-or-minus 5 percent. Well, I've never had the pleasure of working with a team capable of that kind of accuracy, but I've never heard a client complain when I came in below budget, and it's been a long time since an overrun exceeded the buffer I put in my own fixed bids. How do I set my fixed bids? Well, I'm afraid some problems you need to solve on your own. ▮

Larry O'Brien is a technology consultant, analyst and writer. Read his blog at www.knowing.net.

All Aboard the SOA Train

"Our problem was we had applications out there that were coupled, and it was hard to do a release cycle. We'd change one thing, but it touched 20 or 30 other applications. Things were breaking all the time.

"It was a fixed cycle of a moving train. If you jump and miss the train, you have to wait for the next one. But by then, your piece might not be relevant anymore."

Industry Watch

This was the problem that two years ago was facing Vladimir Mitevski, director of product management in core technologies at Thomson Financial, which provides workflow solutions for the financial services industry. He needed to cut development costs and give the organization the ability to respond quickly to new business opportunities and challenges.

Mitevski wasn't sure if Thomson was alone in this problem, so he began to look around at other ways to maintain and update all the company's applications. After weighing all the factors, they embarked on a project around service-oriented architecture. He shared his thoughts in a talk titled "SOA Is Risky for Your Business" at the recent Web Services on Wall Street Show & Conference in New York City.

"The biggest challenge was in our organizational culture," Mitevski said. "There were people working in silos, doing certain things for a long time. Now we come in and break their concept of how to do their jobs, and how to run that part of the business."

A key to making SOA work was to sell senior management on it. But Mitevski pointed out that you can't do that by talking bits and bytes; SOA must be discussed on a conceptual level, and from the point of view of ROI. "We showed the savings in bodies. We said we should be able to fix the problem with X number of bodies, then it would only take one person to execute on the new system, to move things through a release cycle with full visibility and the ability to reverse-engineer."

The pitfall, he noted, was that he had to worry that the business guys would trim his staff, since he showed he could now do the job with fewer people. "It was important to show that we would use the high-level people on high-level tasks. Expensive developers shouldn't be troubleshooting a misplaced comma."

But senior management did buy in, and in a big way. Because the problem at Thomson was so painful, and so intractable, Mitevski said he was basically given a blank check to solve it.

Once he overcame the cultural and senior management impediments, Mitevski still was far from in the clear. He had to train his team on the concept and technology, and make sure he had enough people trained in the right areas to complete the task. After a while, he said, "the team had the correct mindset, but the skills weren't there. If a developer knows C++, he'll solve everything with C++. They lacked an understanding of UDDI and the other services protocols."

Mitevski said the team first tackled the problem with infrastructure, and now "people are starting to piggyback on it." Governance, policy management, and the ability to register more services off mainframes all are being built out, and Thomson has published its own internal standards for services based on the industry standards. "The protocols are so abstract we needed to standardize how they applied to our business," Mitevski said.

Despite the enormity of the task—they basically moved the entire Thomson organization onto the new architecture—Mitevski believes they took the right road.

"It took a lot of coordination with a lot of hand-holding," Mitevski said. "We were still attached to the train, but now with a long, never-ending, stretchable rope."

STILL (LAWSUIT) CRAZY

In speaking with the noted author Ed Yourdon for my piece on the Chaos Report earlier in this newspaper, he mentioned that among his many roles, he often is called to serve as an expert witness at trials involving intellectual property rights and canceled software projects.

Interestingly, Yourdon noted that lawsuits over those failed software projects are as prevalent as they were five years ago, despite the new metrics that show the industry as a whole is doing better at creating software on time, on budget and that meets all the end user's requirements.

He also said he was discouraged to note that the lawsuits are occurring for the same old reasons: bad or vague requirements, constant changes as users can't make up their minds about what they want in the software, and a lack of risk management.

Part of the reason for the continued litigation, Yourdon pointed out, is that fewer large software projects are being done in-house. The suits he sees involve, for example, a Fortune 500 company against IBM Global Services, or EDS. The number of lawsuits "is somewhat surprising," he said. "You'd think we would have gotten better." ▮

David Rubinstein is editor-in-chief of SD Times.

BUSINESS BRIEFS

CA filed its third-quarter 2007 fiscal results and reported revenue of more than US$1 billion. CA president and CEO John Swainson credits strong demand for the company's enterprise IT management solutions for the revenue growth; many of those services were acquired from other vendors during the past two years. Other contributing factors to CA's revenue growth were improved customer retention, growth of new products and services, and a realignment of its sales force, the company reported. Subscription revenue accounted for 77 percent of the quarter's revenue. The filing included pro forma projections for earnings per share from continuing operations of 26 cents to 29 cents and estimates that CA will exceed $3.9 billion in revenue before the year's end . . . **Interwoven**, a purveyor of content management solutions, supplied investors with selected 2006 financial results. Its revenues before interest, taxes and expenses increased 14 percent from US$175.0 million to $200.3 million over the past year. The company's revenue growth was due in large part to the success of its support and services business unit, and uptake in license revenue. It introduced updated versions of its Interwoven WorkSite and Scrittura Messaging products in the fourth quarter. Interwoven's new customer sign-ups in Q4 2006 yielded its most sizable quarterly growth in six years. It now has approximately 3,800 customers worldwide. Cash, cash equivalents and investments increased by $16.1 million in the fourth quarter, to a total of $176.5 million . . . **Enea**, the creator and distributor of the OSE real-time operating system, filed its full-year report for 2006. Its net sales grew by 3 percent over the year to US$726 million; software sales accounting contributed $250 million, growing 9 percent. The company's operating profit increased 20 percent and total operating costs were $3 million. Its profit after taxes was $69 million, and earnings per share totaled 19 cents. Quarterly profit surged 24 percent in the fourth quarter, while software sales accounted for 34 percent of fourth-quarter sales. Its OSE operating system powers nearly half of the world's 3G mobile devices, according to the financial statement. Enea significantly expanded its product portfolio of embedded development tools in 2006, the company also claimed. ▮

EVENTS CALENDAR

EclipseCon — March 5–8
Santa Clara
ECLIPSE FOUNDATION
www.eclipsecon.org/2007

Game Developers Conference — March 5–9
San Francisco
CMP MEDIA
www.gdconf.com

Developer Relations Conference — March 12–13
San Francisco
EVANS DATA
www.evansdata.com/drc

BrainShare — March 18–23
Salt Lake City
NOVELL
www.novell.com/brainshare

SD West — March 19–23
Santa Clara
CMP MEDIA
www.sdexpo.com

VSLive — March 25–29
San Francisco
FAWCETTE TECHNICAL PUBLICATIONS
www.ftponline.com/conferences/vslive/2007/sf

Emerging Technology Conference — March 26–29
Burlingame, Calif.
O'REILLY MEDIA
conferences.oreillynet.com/et2007

Embedded Systems Conference — April 1–5
San Jose
CMP MEDIA
www.embedded.com/esc/sv

Web 2.0 Expo — April 15–18
San Francisco
O'REILLY MEDIA
www.web2expo.com

Gelato ICE Itanium Conference & Expo — April 15–18
San Jose
GELATO FEDERATION
www.ice.gelato.org

Software Security Summit — April 16–17
San Mateo, Calif.
BZ MEDIA
www.S-3con.com

Software Test & Performance Conference — April 17–19
San Mateo, Calif.
BZ MEDIA
www.stpcon.com

CA World — April 22–26
Las Vegas
CA
www.caworld.com

MySQL Conference & Expo — April 23–26
Santa Clara
MYSQL AND O'REILLY MEDIA
www.mysqlconf.com

Microsoft MIX07 — April 30–May 2
Las Vegas
MICROSOFT
visitmix.com

For a more complete calendar of U.S. software development events, see www.bzmedia.com/calendar. Information is subject to change. Send news about upcoming events to events@bzmedia.com.

Software Development Times (ISSN 1528-1965) is published 24 times per year by BZ Media LLC, 7 High St., Ste. 407, Huntington, NY 11743. Periodicals postage paid at Huntington, NY, and additional offices. SD Times is a registered trademark of BZ Media LLC. The price of a one-year subscription is US$179 for subscribers in the U.S., $189 in Canada, $229 elsewhere. POSTMASTER: Send address changes to SD Times, PO Box 2169, Skokie, IL 60076. SD Times subscriber services may be reached at sdtimes@halldata.com or by calling +1-847-763-9692.


ALTOVA®
missionkit™ 2007
Gear up for development excellence
Take off with the Altova MissionKit, and discover the secret to savings on top software tools.
Spied in the Altova MissionKit 2007:
• The world's leading XML development tools
• Plus application design, data management, and modeling options for software architects
The Altova MissionKit 2007 bundles Altova's intelligent application development, data management, and modeling tools at 50% off their regular prices. Available in a variety of configurations tailored to the needs of software architects and XML developers, the Altova MissionKit delivers the highest functionality and best product value. It's your first-class ticket to the power, speed, and simplicity of Altova's award-winning product line. Save a bundle!
Download the Altova MissionKit 2007 today: www.altova.com
Supports official new W3C standards: XSLT 2.0, XPath 2.0 & XQuery!
ALTOVA®


Ship Software OnTime!
(watch the video or download the free software at axosoft.com/sdtimes)
Are You Trending Toward Zero Defects?
axosoft
OnTime 2007
bug tracking • requirements management • helpdesk
for agile, scrum and extreme development teams